TCRS 1/2025

Teoria e Critica della Regolazione Sociale

MIMESIS

CYBERSECURITY
E ISTITUZIONI DEMOCRATICHE
UN'INDAGINE INTERDISCIPLINARE: DIRITTO, INFORMATICA E ORGANIZZAZIONE AZIENDALE

Fascicolo II

A cura di/Edited by
Paolo Heritier e Stefano Rossa

Introduzione di Riccardo Ursi

La presente pubblicazione è finanziata dal Bando Ricerca UPO 2022 a valere su risorse Next Generation EU e Compagnia di San Paolo, in quanto realizzata nell'ambito del progetto "Cybersecurity Risk Governance in Public Administration – CybeR-GoPA" (ID: 1083758, CUP: C15F21001720001), componenti Prof. Roberto Candiotto, Prof.ssa Lavinia Egidi, Prof.ssa Bianca Gardella Tedeschi, Prof. Paolo Heritier, Dott. Stefano Rossa (responsabile scientifico). Si precisa che il Dott. Stefano Rossa è ricercatore t.d. con contratto finanziato da Commissione Europea – FSE REACT-EU, PON Ricerca e Innovazione 2014-2020 – CUP C65F21001410001. Volume pubblicato con il contributo dell'Università del Piemonte Orientale, Dipartimento per lo Sviluppo Sostenibile e la Transizione Ecologica.

Tutti i contributi del presente volume, ove non diversamente esplicitato in nota, sono stati sottoposti a procedura di doppio referaggio cieco.

Mimesis Edizioni (Milano – Udine)
www.mimesisedizioni.it
mimesis@mimesisedizioni.it

Issn: 1970-5476
Isbn: 9791222320793

Piazza Don Enrico Mapelli, 75
20099 Sesto San Giovanni (MI)
Phone: +39 02 24861657 / 21100089

Registrazione presso il Tribunale di Milano n. 299 del 23-10-15

Indice

Riccardo Ursi

Introduzione. La sicurezza cibernetica come funzione pubblica[*]

I cambiamenti imposti dal rapido sviluppo tecnologico dell'ultimo trentennio richiedono oggi di affrontare il tema della sicurezza cibernetica partendo da una nuova prospettiva in chiave strettamente giuspubblicistica, richiedendo di inquadrare il fenomeno anche (e soprattutto) come una funzione pubblica. L'emergere di questa inedita prospettiva ha messo il giurista dinanzi a questioni nuove e particolarmente complesse, in quanto lo studio del fenomeno richiede una riflessione sulla nozione stessa di cybersicurezza (nonché, a monte, della stessa definizione di sicurezza). Il concetto di *cybersecurity* oggi non può che essere inteso in modo da coinvolgere non solo le mere attività di gestione e prevenzione dei rischi interni al cyberspazio, ma sembra coinvolgere indistintamente la dimensione virtuale così come quella reale. Del resto, se da un lato l'evoluzione delle reti informatiche globali hanno premesso un progresso notevole sul piano economico e sociale di tutte le principali democrazie occidentali, dall'altra la stessa ha esposto individui, imprese e istituzioni a rischi significativi. In questo contesto, il giurista è chiamato a traslare categorie giuridiche tradizionali all'interno di un di uno spazio non legato a confini geografici, un 'non luogo' in cui gli Stati-nazione – nonostante i più strenui tentativi in senso contrario – si sono trovati privati della possibilità di esercitare la loro sovranità. Il compito di cura della sicurezza cibernetica affidato alle istituzioni pubbliche nazionali ed europei richiede così agli studiosi del nuovo millennio di affrontare con lenti nuove alcuni temi di centrale rilievo dal punto di vista teorico e pratico.

Questo numero monografico si propone l'ambizioso obiettivo di esplorare alcune tra le questioni trasversali più rilevanti nell'attuale dibattito che sta interessando la materia. L'interrogativo probabilmente più rilevante, rivolto a comprendere come possa lo Stato garantire la sicurezza dei suoi cittadini rispetto ai pericoli provenienti dal ciberspazio in assenza di un controllo diretto sul fenomeno da cui proviene il rischio, sembra allo stato dell'arte destinato a rimanere privo di una risposta soddisfacente. Se i tentativi di risposta a tale interrogativo appaiono oggi tutt'altro che soddisfacenti, in questa prima fase di studi della materia risultano già ben definiti quelli che sono i principali interrogativi che i giuristi – accompagnati da studiosi e operatori di altre materie – sono chiamati a svolgere. Tra questi, senza alcuna pretesa di esaustività, risulta inevitabile interrogarsi sulle seguenti questioni

* Scritto non sottoposto alla procedura di referaggio doppio cieco.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760156

messe a fuoco nelle successive pagine: (*i*) il concetto di sicurezza cibernetica può essere riferito allo stesso concetto di 'sicurezza' tradizionalmente affrontato dalla scienza giuridica italiana (ammesso che ne esista uno univoco)?; (*ii*) qual è il rapporto tra ordinamento nazionale ed europeo nel nuovo ordinamento multilivello di *cybersecurity*?; (*iii*) come prima ricaduta, qual è il rapporto tra sicurezza cibernetica e nazionale?; (*iv*) come seconda ricaduta, quale spazio può essere affidato ai provati attraverso forme di partenariato in una materia legata a doppio filo con informazioni classificate?

Alla luce di tali quesiti, risulta necessario ridefinire il ruolo dello Stato e delle istituzioni pubbliche, sia a livello nazionale che sovranazionale, in relazione alla tutela della cybersicurezza. La crescente interdipendenza tra sistemi informatici e infrastrutture critiche ha reso evidente che la protezione dello spazio cibernetico non può essere più ricondotta al tradizionale binomio tra sicurezza interna e sicurezza esterna, ma deve essere affrontata attraverso nuove categorie, prima tra tutte quelle di 'ordine pubblico globale'. Lo Stato, in questo senso, non assume più soltanto il ruolo di garante della sicurezza fisica, ma è chiamato a essere il custode della sicurezza digitale, con la responsabilità di proteggere cittadini, imprese e infrastrutture dall'invisibile minaccia cibernetica.

Tuttavia, questo compito è complicato dal fatto che le tecnologie digitali si sviluppano in un ambiente globale e decentralizzato, rendendo difficile per gli Stati esercitare il loro tradizionale monopolio del potere coercitivo. Di fronte alla complessità e alla globalità delle minacce cibernetiche, che spaziano dagli attacchi informatici alle violazioni della privacy, si richiede una nuova architettura di governance multilivello. Tale architettura deve necessariamente includere non solo le autorità pubbliche, ma anche gli attori privati, le organizzazioni internazionali e la società civile.

In questo contesto, la collaborazione tra pubblico e privato diventa essenziale. Le imprese, infatti, detengono molte delle risorse tecnologiche e delle competenze necessarie per affrontare le sfide della cybersicurezza, mentre lo Stato possiede la legittimità e la capacità di coordinare e regolamentare le attività di difesa del cyberspazio. Il modello emergente sembra quindi orientarsi verso un sistema di (cyber-)resilienza in cui Stato e attori privati cooperano attivamente per prevenire, mitigare e rispondere agli attacchi cibernetici.

Inoltre, la dimensione europea della cybersicurezza ha acquisito sempre maggiore rilevanza, con l'Unione Europea che ha adottato un ruolo di primo piano nella definizione di politiche e regolamentazioni comuni. Con l'adozione del più recente pacchetto legislativo in materia, e con particolare riferimento alla direttiva (UE) 2022/2555 (nota come direttiva NIS2) l'Unione ha delineato un quadro giuridico che mira a innalzare notevolmente il livello minimo di sicurezza delle reti e delle informazioni in tutto il territorio europeo. La sfida non è più quella di una mera armonizzazione tra le differenti legislazioni nazionali, ma quella di ottenere dei benefici comuni attraverso l'istituzione di infrastrutture comuni e di forme di cooperazioni tra Stati membri. La sfida è sicuramente ambiziosa, in quanto è rivolta a trovare un delicato punto di equilibrio tra l'infrastruttura verticale, riferita ai rapporti tra UE e singoli Stati, e orizzontale, riferita al rapporto tra pubblico e

privato, con l'obiettivo di individuare una formula di azione il quanto più possibile efficace. Tuttavia, poiché i soggetti chiamati a sostenere i costi dell'intera infrastruttura europea risultano oggi in larga parte coincidenti con gli stessi onerati ad adempiere ai diversi obblighi previsti dall'attuale architettura livello di cibersicurezza, l'attuale sistema non può che sollevare diverse perplessità circa il sostegno che il settore pubblico dovrà fornire per raggiungere gli obiettivi minimi prefissati.

Negli ultimi trent'anni la crescita di Internet e dell'innovazione che ne è derivata è stata facilitata da un ambiente relativamente privo di controlli. Tuttavia, la profonda integrazione nel quadro sociale del *World Wide Web* ha messo in discussione l'idea tradizionale di sicurezza, intesa come predisposizione di un perimetro normativo funzionale al libero esplicarsi della sfera individuale. Ad essa sembra progressivamente sostituirsi un modello legato al concetto di protezione, caratterizzato dalla disponibilità (anche implicita) a scambiare/sacrificare spazi di libertà personale a fronte della possibilità di operare in un ambiente sociale e tecnologico politicamente e giuridicamente protetto (secondo il paradigma dello Stato preventivo)[1].

In questo contesto, per poter affrontare il tema della dimensione giuspubblicistica della sicurezza cibernetica occorre svolgere una ricostruzione che non operi un semplice adattamento delle categorie tradizionali, ma che cerchi di elaborarne di nuove. La vocazione libertaria dello spazio virtuale, frutto della circostanza che esso è, in ultima analisi, il prodotto più rappresentativo di forme estreme di anarco-liberalismo individualista, mal tollera i paradigmi dello Stato westfaliano, sovrano e regolatore, ma dà la stura al consolidarsi di un governo ampiamente nelle mani di poteri privati, senza ricevere la legittimazione di istituzioni nazionali o sovranazionali[2]. Queste ultime cercano di inseguire uno sviluppo tecnologico incontrollato attraverso strumenti di regolazione, più o meno vincolanti, e attraverso attività amministrative e giudiziarie che mirano rivendicare spazi di sovranità ed esercizio di poteri pubblici[3]. L'obiettivo non è solo l'autoconservazione dello Stato e delle sue componenti, ma soprattutto la sicurezza degli individui, dei gruppi e delle entità economiche e sociali in una logica neo-hobbesiana.

Adattando allo spazio cibernetico questo assunto si potrebbe dire che, senza una rete protetta da pericoli e minacce, al giorno d'oggi anche la vita degli individui è priva di prospettive certe. Cosa si intende per rete sicura, in che modo il Leviatano può ancora svolgere il suo ruolo in un mondo senza confini, in che senso il diritto può regolare l'azione dei privati e i compiti delle istituzioni pubbliche, sono questioni che si intersecano nella delimitazione del concetto giuridico di sicurezza cibernetica. In proposito, si potrebbe individuare una nozione ampia, che riguarda il livello sociale-cognitivo ovvero l'insieme delle relazioni umane e delle caratteristiche socio-cognitive, e una nozione ristretta, che riguarda la protezione del livello fisico-infrastrutturale e del livello logico-informativo. Nel primo caso la

1 Pizzolato 2017: 39.
2 Mannoni e Stazi 2021: 24.
3 Betzu 2021: 24.

sicurezza attiene alla protezione dei beni giuridici che vengono lesi direttamente dall'uso degli strumenti informatici e che vedono il cyberspazio come ambiente delle condotte lesive nei confronti degli individui; nel secondo caso la sicurezza riguarda precipuamente le aggressioni alle infrastrutture ed ai sistemi informatici il cui effetto è, in varia misura, la lesione di beni giuridici fisici.

In entrambi i casi, i problemi giuridici della sicurezza cibernetica attengono alle modalità di repressione e, soprattutto, di prevenzione delle condotte lesive, ai soggetti, pubblici e privati, investiti della funzione di garantire la sicurezza, ai poteri correlati a tale funzione, nonché alle fonti di regolazione.

Con riferimento alla sicurezza cibernetica in senso ampio, correlata ad una idea di ordine pubblico digitale, il tema riguarda l'attività di repressione degli illeciti e di prevenzione delle condotte lesive, che impongono una rivisitazione delle categorie tradizionali del diritto penale e spingono inevitabilmente ad immaginare un ambito operativo di interrelazioni tra forze dell'ordine e autorità di sicurezza che esorbita i confini statuali. Si tratta di attività amministrative e giudiziarie espressioni di poteri sovrani, la cui efficacia risulta pregiudicata dalla collocazione territoriale dell'autore di simili illeciti, ammesso che lo si possa individuare, e dal fatto che l'intermediario privato che gestisce la rete ha la disponibilità esclusiva dei dati e dei contenuti sui quali si intende intervenire. In questa prospettiva, soggetti privati, titolari di piattaforme e *providers,* esercitano poteri preventivi e sanzionatori nei confronti dei propri utenti, spesso in maniera sommaria e senza alcuna garanzia procedurale.

Si è pertanto in presenza di un quadro complesso in cui, a fronte di una incrementale domanda di sicurezza generata dai pericoli e dalle minacce provenienti da un mondo virtuale, si registra un indebolimento delle tradizionali funzioni pubbliche statuali e una loro contaminazione forzata. E ciò in quanto il mondo socio-politico ha delegato al mondo privato-imprenditoriale il disegno e la gestione dell'architettura cibernetica, la quale integra una dimensione della sicurezza avulsa dalle categorie giuridiche di cui si è sempre nutrita, ossia la legittimazione, la polarità privato-pubblico, il nesso di spazialità-territorialità.

La protezione *nello* spazio cibernetico si è altresì sviluppata nell'idea della protezione *dello* spazio cibernetico, o meglio di quella porzione che influenza l'ambito degli interessi pubblici considerati rilevanti e vitali per la loro dimensione fisica. In tal senso, l'ordine pubblico digitale viene declinato come protezione degli interessi minacciati da condotte lesive nei confronti dei sistemi e delle reti informatiche: un ambito che coinvolge l'insieme delle tecnologie e delle misure di risposta e mitigazione progettate per tutelare reti, *computer*, programmi e dati da attacchi, danni o accessi non autorizzati, in modo da garantire riservatezza, integrità e disponibilità. Ed è proprio tramite la individuazione degli interessi primari da proteggere che la sicurezza cibernetica si presenta come una funzione pubblica, la quale muovendo da un controllo delle infrastrutture tecnologiche tenta di inibire pericoli e minacce sulle persone.

I criminali informatici sono ormai in grado di sfruttare le vulnerabilità dei prodotti e delle reti informatiche per acquisire illegalmente i dati che transitano nello spazio cibernetico e per compromettere, in tutto o in parte, il funzionamento di

servizi o sistemi digitali: è sotto questa prospettiva che la sicurezza cibernetica emerge come prestazione di un servizio essenziale per il mantenimento di attività civili, sociali ed economiche fondamentali dello Stato. Come è stato osservato, «l'ampia gamma di azioni ostili può andare dallo spionaggio agli attacchi veri e propri, con finalità di inibire, alterare o addirittura distruggere dati, *hardware*, reti o eventuali servizi e sistemi ad essi connessi. Generalmente possono essere rivolte ad assetti governativi, economico-finanziari, imprese, infrastrutture critiche o servizi dedicati alla società civile. I possibili effetti da essi generati possono facilmente divenire strategicamente rilevanti oppure influenzare comportamenti, azioni e documentazione collegati anche ad operazioni militari in corso. I protagonisti possono essere entità statuali, gruppi terroristici, organizzazioni criminali o semplici individui dediti alla ricerca di informazioni o alla distruzione/danneggiamento dei sistemi informatizzati e dei dati in essi contenuti»[4]. Si tratta, dunque, di una funzione di sicurezza che interessa, complessivamente, l'ordinamento statale e, in dettaglio, le sue componenti, ossia le imprese e i singoli cittadini. Da questo punto di vista, «la tecnologia non soltanto ha offerto in tempi particolarmente brevi eccezionali occasioni di progresso e quindi di sviluppo delle possibilità di conoscenza, di miglioramento culturale, sanitario, tecnologico, economico, ma ha ad un tempo consentito l'affermarsi di modalità aggressive che, se operate con propositi criminali, sono in grado di minacciare sia gli interessi dello Stato che la fruibilità dei diritti dei soggetti di un ordinamento»[5].

In definitiva, sussiste un interesse pubblico che denota una funzione statuale: quello di apprestare, contestualmente, mezzi di protezione a favore dello Stato e dei suoi soggetti, relativi alla sopravvivenza, all'incolumità e all'integrità politica, alla stabilità economica e al benessere sociale derivanti dall'utilizzo dello spazio cibernetico. In questa prospettiva, si fa strada una dimensione più ristretta della sicurezza cibernetica, che ha una duplice natura: la difesa del "fortino" tecnologico, che protegge quegli interessi di fronte ad attacchi tesi a minarne la stabilità; l'attività di prevenzione, che si coagula nella promozione della resilienza delle infrastrutture rispetto al pericolo, potenziale o attuale, di pregiudizio al funzionamento delle stesse, al fine di inibire o mitigare i danni alle persone, alle imprese di settori nevralgici per la vita economica, o alle istituzioni democratiche. La funzione amministrativa connessa all'ordine pubblico digitale diventa allora l'organizzazione e la raccolta di risorse, processi e strutture volte a proteggere il cyberspazio e i sistemi abilitati da eventi pregiudizievoli[6], al fine di tutelare interessi considerati rilevanti anche ai fini della sicurezza nazionale.

Al riguardo, si deve osservare come la fluidità della rete senza confini non consente di precisare i tratti distintivi tra attività di difesa, ossia protezione dalle minacce esterne, e attività di sicurezza, volta a garantire in termini preventivi l'incolumità di persone e beni[7].

4 Cfr. De Felice 2012: 72.
5 De Vergottini 2019: 76.
6 Craigen, Daikun-Thibault, Purse 2014: 17.
7 Lauro 2021: 530.

Di fronte alla fisiologica a-territorialità dello spazio cibernetico si individua una sorta di *area di territorializzazione effettuale* dello stesso, in modo da definire un ambito di tradizionale autorità ed esercizio dei poteri correlati: una funzione di tutela che si lega alla natura nazionale (e quindi direttamente o indirettamente territoriale) degli interessi tutelati[8]. Tale funzione è contrassegnata, da una parte, dal carattere dinamico della stessa, derivante dalle continue interazioni tra esseri umani e sistemi informatici, e dall'altra, dalla sua complessità intrinseca, in quanto immaginata per fornire protezione nei confronti dell'intera gamma degli eventi pregiudizievoli, siano essi intenzionali ovvero accidentali. In questo senso, la funzione di sicurezza cibernetica si dettaglia: nella creazione di un modello organizzativo complesso e policentrico, idoneo a monitorare e sorvegliare il "fortino"; nel rafforzamento dei potenziali bersagli vulnerabili, consentendo loro di resistere agli attacchi o di impedire le intrusioni; nel costruire sistemi resilienti in grado di continuare a funzionare durante un attacco, riprendersi rapidamente ed, eventualmente, rispondere agli attaccanti.

Ciò posto, si potrebbe ritenere che il concetto di sicurezza cibernetica in senso stretto compendi due tipi di attività di rilievo pubblico: la *cyber-defense*, intesa come resistenza di fronte ad un attacco informatico, e la *cybersecurity*, intesa come prevenzione e resilienza del sistema informatico rispetto ad un potenziale attacco.

In definitiva, se la difesa del "fortino" informatico si muove, sul piano oggettivo e soggettivo, lungo le linee della funzione di sicurezza nazionale e della difesa militare, l'attività di prevenzione, volta a garantire la resilienza del sistema informatico rispetto a potenziali minacce, rappresenta una funzione nuova per la quale si individua un compito pubblico, nel quale regolazione e amministrazione assumono connotati peculiari, e una architettura organizzativa, che si contraddistingue per un modello composito in cui convivono soggetti pubblici dotati di poteri autoritativi e forme di cooperazione con soggetti privati.

I contributi inserito all'interno di questo fascicolo, seguendo lo spesso spirito delle relative relazioni tenutesi dagli Autori al Convegno ospitato dall'Università del Piemonte Orientale di Novara, sono stati raccolti e ordinati seguendo l'idea – che si spera che possa rimanere ferma nei successivi studi – dell'eclettismo come indispensabile obbligo metodologico. Senza un reciproco interesse tra la componente tecnica e quella propriamente giuridica della materia, la sicurezza cibernetica è destinata a rimanere un corpo in tutto o in parte estraneo nel proprio campo di studio.

Bibliografia

Betzu M. 2021, *I baroni del digitale*, Napoli: Editoriale Scientifica.

Craigen D., Daikun-Thibault N., Purse R. 2014, "Defining Cybersecurity", in *Technology Innovation Management Review* (10) 17.

8 Tsagourias 2015: 21.

De Felice N. 2012, "Strategia di difesa nel cyberspazio quale contributo alla tutela degli interessi nazionali", in U. Gori, L.S. Germani (a cura di), *Information warfare 2011. La sfida della cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano: Franco Angeli, 72.

De Vergottini G. 2019, "Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata", in *Rivista AIC* (4) 76.

Lauro A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *Gruppo di Pisa*, (3) 530.

Mannoni S., Stazi G. 2021, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli: Editoriale Scientifica.

Pizzolato F. 2017, "Il costituzionalismo alla prova della tecnica: libertà, uguaglianza e sicurezza", in F. Pizzolato, P. Costa (a cura di), *Sicurezza e tecnologia*, Milano: Giuffré.

Tsagourias N. 2015, "The legal status of cyberspace", in Tsagourias N., Buchan R. (eds.), "*Research handbook on International Law and Cyberspace*, Cheltenham: Edward Elgar Publishing, 21.

Giovanni Bombelli

Dogmatica, certezza e (in)calcolabilità. Note su profili di "anticipazione cognitiva" in tema di legal design *e* decision-making

Abstract: Partendo dal rapporto tra sicurezza e modernità, il saggio si concentra su alcuni aspetti riguardanti la nozione di "cybersecurity" e, in particolare, il legame tra cybersecurity-intelligenza artificiale-dogmatica giuridica. Alla luce di questo quadro, viene discussa la possibilità e la plausibilità di un "approccio cognitivo" (cioè di anticipazione cognitiva) al diritto, con particolare attenzione ai concetti di "legal design" e "decision-making" anche considerando i molteplici riflessi provocati dalle mutazioni tecnologiche sulla dogmatica giuridica. Più in generale, la questione coinvolge la natura del rapporto sfera giuridica-universo digitale e l'inevitabile connessione tra il diritto e le altre scienze

Keywords: Dogmatica giuridica, Certezza, Anticipazione cognitiva, Legal design, Decision-making.

1. Premessa

Nelle pagine seguenti si proporranno alcune riflessioni, da intendersi come mere linee di osservazione, situate a cavallo di fenomenologia sociale attenta alle dinamiche socio-tecnologiche e teoria del diritto.

Senza ambire all'elaborazione di "quadri" o "soluzioni" definitivi, a partire da una prospettiva filosofico-giuridica l'obiettivo è offrire una serie di impressioni che attengono all'universo complesso e inevitabilmente cangiante delle mutazioni tecnologiche in atto e della relativa disciplina normativa.

In questa direzione, si proverà ad articolare un quadro critico strutturato secondo cerchi concentrici. Dopo alcune note introduttive relative al nesso che intercorre tra (cyber)sicurezza e modernità, ci si soffermerà su qualche profilo di carattere generale che attiene alla "cybersicurezza". Ciò consentirà di appuntare meglio l'attenzione sul circuito che intercorre tra quest'ultima, l'intelligenza artificiale e la dogmatica giuridica, con particolare riguardo alla plausibilità del configurarsi di un modello di "anticipazione cognitiva" (o cognitivo-normativa) in tema di *decision-making* e *legal design*.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760157

Per questa via si addiverrà ad alcune notazioni conclusive, con particolare riguardo alla progressiva compromissione della grammatica concettuale e categoriale di matrice moderna determinata dalle mutazioni tecnologiche in atto e dal connesso *framework* normativo vieppiù connotato da forme di *multilevel regulation*: ciò aprirà ad un interrogativo finale relativo al nesso che intercorre tra sfera giuridica e universo digitale, che convoca orizzonti concettuali in qualche misura interdisciplinari.

2. (Cyber)Sicurezza e modernità

Il tema della cybersicurezza chiama in causa il rapporto con le coordinate teoriche che informano la modernità giuridica e la relativa dogmatica.

Più precisamente, viene a tema il nesso concettuale che si istituisce tra la dimensione sicuritaria[1], come luogo teorico classicamente filosofico-giuridico di cui la dizione "cybersicurezza" costituisce una sorta di proiezione contemporanea, l'apparato teorico-concettuale sotteso all'elaborazione del giuridico e il modello di Stato. Un trinomio che informa le grammatiche moderne della sicurezza e da riprendere, in conclusione, con riguardo al grado di funzionalità e legittimità degli odierni assetti democratici.

In questa direzione, il paradigma o termine di confronto critico non può che essere rappresentato dalla prospettiva di Thomas Hobbes. Di essa si richiamano solo due versanti tra loro connessi in quanto appaiono particolarmente funzionali alla riflessione qui proposta: a) la struttura del dispositivo statuale e b) il binomio *safety-security*. Esaminiamoli distintamente.

a) Con buona approssimazione, si può affermare che lo Stato moderno nasca per garantire "sicurezza". Essa, infatti, ne rappresenta una sorta di costante individuando, per molti versi, la cifra essenziale del nuovo soggetto politico-istituzionale inauguratosi al tramonto dell'epoca medievale.

Una dimensione, quella della sicurezza, che appare giocata su due livelli del perimetro statuale: interno e esterno.

Essa viene intesa sin da subito come "sicurezza interna" allo Stato, radicata nella coppia pubblico-privato. Come concettualizzato originariamente da Hobbes, l'edificazione del potere statuale in termini di *pacta* a base territoriale, coincidente con la sfera "pubblica" e fondato sul riconoscimento reciproco dei soggetti in quanto contraenti, appare funzionale sia a predisporre forme di controllo sociale sia, al contempo, a tutelare la sfera individuale o "privata" colta come piano simmetrico allo spazio pubblico[2].

1 In merito, per un quadro generale, *ex multis* Pizzolato, Costa 2015; Cocco 2012; Greco 2009. Per un *focus* sulla realtà della "città" Buzzacchi, Costa, Pizzolato 2019.

2 Per un'articolazione più distesa di questi passaggi concettuali si consenta rinviare a Bombelli 2015a: 53-54 in particolare. Ivi il rinvio a Hobbes 2001 [1651], Parte I, XIV, 9-11; nel testo appena citato si veda anche la nota 19 riguardo al binomio *fear-trust/faith* operante nella riflessione del filosofo inglese (il riferimento è alla edizione italiana del 2001: 218-220).

Tale plesso tematico riposa, a sua volta, su un modello di calcolabilità strutturalmente connesso alla certezza del diritto. in altre parole, il paradigma teorico vive sulla possibilità di "calcolare", nel senso di pianificare o prevedere-anticipare a livello cognitivo, le dinamiche sociali interne allo Stato, mentre l'orizzonte della certezza verte sulla particolare configurazione in termini di certezza conferita (*rectius*: che si pretende di conferire) al diritto. Storicamente ciò si rende possibile in ragione dell'unificazione delle fonti allestita in capo al sovrano e conseguente al processo di affermazione dell'impianto statuale: in altre parole, lo Stato moderno nasce "sicuro" in quanto reso "calcolabile" attraverso il ricorso all'unificazione del diritto inteso come strumento di certezza.

Diverso il quadro "esterno" all'area statuale che, in qualche misura, permane impregiudicato. Alla reale (o, quantomeno, auspicata) sicurezza intra-statuale fa infatti da contraltare lo scenario dei rapporti inter-statuali, ove l'orizzonte del perimetro territoriale funge da mero discrimine tra i nuovi attori interessati (gli Stati).

Se la pace di Vesfalia segna notoriamente un passaggio decisivo nell'istituire le regole che disciplinano tale scenario, al contempo essa non appare in grado di ergersi a regola invalicabile. In tal senso, il principio del *pacta sunt servanda*, in cui si sintetizza l'esito nucleare del trattato del 1648 e il contenuto essenziale del nascendo diritto internazionale, rappresenta un riferimento normativo sempre suscettibile di una ridiscussione radicale. In altre parole, sottraendosi alle forme di controllo giuridico predisposte dalla modernità per il contesto statuale a base territoriale[3], la sicurezza inter-(extra)statuale si configura in termini strutturalmente "in-calcolabili".

b) Come segnalato, nella riflessione hobbesiana il tema della sicurezza, nella sua duplice declinazione intra-statuale e extra-statuale, si intreccia con il binomio *security* e *safety*. Un binomio che il teorico inglese sviluppa segnatamente con riguardo all'orizzonte intrastuale secondo tonalità invero un poco ambigue.

Per un verso, infatti, la sicurezza va intesa come "preservazione" delle condizioni esterne di convivenza e, quindi, in funzione del controllo della sfera individuale: in altre parole, come modello di *security* nel quadro dell'architettura concettuale richiamata al punto precedente.

Al contempo, il tema sicuritario rinvia ad altra area semantica. Da questa prospettiva, esso emerge in termini di *safety* (quasi come forma di sicurezza "interna" o intraindividuale): la funzione di controllo politico attribuita al Leviatano comporta, infatti, che su quest'ultimo gravi altresì l'onere di provvedere al "bene" dei consociati (secondo la dizione *Good-Safety* nella versione inglese del testo hobbesiano, *salus* nella versione latina)[4]. Esso potrebbe intendersi come "sviluppo delle potenzialità" dei singoli consociati: in altre parole, un modello orientato al *flourishing* individuale e collettivo che, in modo solo apparentemente paradossale nel

3 Sul punto ineludibile la menzione di Schmitt 1991 [1974], su cui ancora Bombelli 2015a: 60. Per una contestualizzazione più ampia si consenta, altresì, rinviare a Bombelli 2018: 5-65.

4 Sul punto Bombelli 2015a: 70 (in particolare la nota 56).

quadro della prospettiva del filosofo di Malmesbury, inaugura una sorta di forma embrionale di *Welfare State*[5].

Di là dalle possibili letture che si possono offrire dell'impostazione hobbesiana[6], su cui in questa sede non interessa soffermarsi, si possono trarre almeno tre corollari.

In primo luogo, la polarità sicurezza interna/esterna originatasi a partire dal filosofo inglese permane sino allo scenario contemporaneo. A ben vedere, essa in qualche modo viene progressivamente potenziata in rapporto al processo di edificazione dell'impalcatura statuale trasfondendosi in una vera e propria dogmatica giuridica ad impronta sicuritaria.

Tale dogmatica, in secondo luogo, mira all'ideale rappresentato dalla certezza del diritto o, per dirla con Natalino Irti, della sua calcolabilità[7]. Per questa via, si istituisce la corrispondenza biunivoca tra "norma certa" e "norma calcolabile": più precisamente, la norma è pensabile come "certa" *in quanto* "norma calcolabile". Ciò, si badi, sul presupposto che si dia uno spazio sociale o pubblico, quindi giuridico-normativo rappresentato dallo Stato a base territoriale, controllabile e "dominabile".

Occorre, infine, sin da ora rimarcare come il gioco del binomio *safety-security* si riproponga sul terreno specifico della tutela della sfera individuale: un versante su cui si tornerà variamente nelle pagine seguenti e in conclusione, con riguardo ai contesti odierni pervasivamente connotati da forme di cybersicurezza.

In sintesi. Il trinomio modernità-dogmatica giuridica-certezza/calcolabilità si costruisce e si dispone *en masse*, proprio a partire dal tema della sicurezza (e, con lessico odierno, cybersicurezza), plasmandosi come una sorta di apparato concettuale che, più ampiamente, può fungere da griglia di lettura del contesto moderno e contemporaneo.

3. Cybersicurezza: alcuni profili

Alla luce del quadro storico-concettuale proposto, si orienta ora l'attenzione sul tema specifico della cybersicurezza.

Nel quadro di uno scenario complesso e strutturalmente mutevole, in merito come noto è andato fiorendo un dibattito articolato e arricchito da un'ampia bibliografia[8] a partire dalla definizione stessa della nozione di "cybersicurezza (nella dizione anglosassone ormai invalsa: cybersecurity)"[9].

5 Questo profilo è stato messo particolarmente in luce da uno storico delle dottrine politiche: Galli 1989: 105-106. Tra l'altro, Galli osserva che Hobbes propone "uno Stato che sembra precorrere le leggi antitrust e il Welfare State propugnati dalle correnti progressiste del XX secolo" (inoltre Galli 1995, cap. 2: 42, con riferimento a Carl Schmitt).

6 Per un quadro generale ancora utile Pacchi 2004.

7 Con ovvio rinvio a Irti 2016.

8 A mero titolo di esempio si segnalano Cortesi 2019; Casadei, Pietropaoli 2021; Faini, Pietropaoli 2021, in particolare cap. 5 *Società tecnologica e istituzioni pubbliche. L'amministrazione digitale e aperta*; Ziccardi 2022 (segnatamente il cap. XIV).

9 Si è così passati dalla "sicurezza informatica intesa come Computer Security [n.d.r. protezione del sistema informatico]" ad una "visione della sicurezza maggiormente orientata

In tal senso, muovendo da una prospettiva filosofico-giuridica si proverà solo a stagliare alcuni aspetti di tale groviglio all'incrocio di prassi e teoria e che, richiamandosi circolarmente, appaiono maggiormente conferenti con quanto si va ragionando.

Più precisamente, si orienterà l'attenzione sul nesso tra "sicurezza" e configurazione dei modelli sociali, sul tema dell'autonomia individuale e, infine, sul reticolo normativo[10] originatosi intorno alla cybersicurezza.

L'orizzonte della "sicurezza" rappresenta un nodo centrale nello strutturarsi dei modelli sociali. Esso, però, va valutato alla luce del rimescolamento in essere delle categorie giuridiche maturate, come appena richiamato, nella modernità, segnatamente con riguardo al cruciale binomio "pubblico"-"privato".

Si pensi, a titolo paradigmatico, alle "cyberwars"[11]. Esse rappresentano una delle proiezioni maggiormente rilevanti dei temi di cui si va dicendo, soprattutto alla luce dell'odierno scenario europeo e mondiale: sotto questo profilo, ciò che connota i conflitti "virtuali" (*rectius* combattuti per via tecnologica) è proprio una sorta di compromissione *in progress* della linea di distinzione elaborata agli albori della modernità tra ambito "privato" e sfera "pubblica". Detto in altri termini: tra individuo e Stato, inteso quest'ultimo *à la* Weber come depositario dell'esercizio della forza tradizionalmente legato al ricorso a strumenti formalizzati e riconoscibili (ad esempio gli eserciti) [12].

alla protezione delle informazioni e dei dati, la c.d. Information Security", sino a introdurre (sotto l'impulso della c.d. Cybersecurity Strategy propugnata dall'Unione europea a partire dal 2013 con il documento "Strategia dell'unione europea per cybersecurity: un ciberspazio aperto e sicuro") la nozione di Cybersecurity funzionale "a denotare che gli interessi da proteggere riguardano oggi le infrastrutture di uno Stato, lo sviluppo delle reti e, più in generale, la sicurezza nel ciberspazio inteso come ambiente complesso di interazione tra persone, software e servizi": Brighi 2021: 135-147, in particolare 135-136 (neretti e corsivi nel testo; a tale contributo si rinvia anche per un quadro sintetico relativo alla disciplina della sicurezza informatica nell'ordinamento giuridico comunitario: 144-147).

10 Sul delinearsi di un reticolo normativo insiste, ad esempio, Golisano 2022: 824-834, circa l'accelerazione nelle politiche di innovazione digitale derivante dal PNNR (Piano Nazionale di Ripresa e Resilienza) e la riallocazione delle competenze amministrative in materia di transizione digitale con la loro concentrazione in capo alla Presidenza del Consiglio dei ministri.

11 In merito, ad esempio, Giannuli, Curioni 2019. Il punto si può correlare ad un orizzonte socio-culturale più ampio e dominato da una sequenza temporale di *shocks*: Giaccardi, Magatti 2022 particolare Parte prima, cap. 2 *Entropia, antropia, shock*.

12 Si pensi, per stare ad alcune vicende recenti, all'intersecarsi di soggetti privati e pubblici (o meglio politici). Un profilo riemerso, proprio con riguardo al ricorso a strumenti tecnologici in contesti bellici, in rapporto a figure come quella di Elon Musk e alla relazione tra alcune sue iniziative imprenditoriali (la cosiddetta "Starlink") e alcuni assetti governativi nel quadro del conflitto Russia-Ucraina. A ciò si può aggiungere la questione recentissima legata alla *startup* cinese "Deepseek" con i relativi precipitati in ordine alle forme di controllo sociale e, più ampiamente, in prospettiva geopolitica. In merito vale la pena soffermarsi, in particolare, sulla "teoria delle due piscine" e sul suo progressivo superamento come ben sintetizzato in Macrì 2024: 17-22, segnatamente 17-18: "Nel periodo 2012-2014, quando si prepara la prima direttiva NIS, era accettata la «teoria delle due piscine». La metafora, definita «tanto semplice quanto arrogante», si riferisce alle strutture che mettono a disposizione dei loro clienti due differenti piscine: una di profondità, dove nuotano gli adulti, e un'altra, bassa, per i bambini. Mentre i Paesi come

In questa direzione viene allora a tema la sfera dell'autonomia individuale, come luogo teorico strutturalmente appartenente alla riflessione moderna e che, da Hobbes e Locke, arriva sino ai giorni nostri.

Si tratta di un profilo decisivo. Intorno a tale coordinata, infatti, viene a tracciarsi il perimetro dell'intervento normativo che, lungo la linea del binomio *safety-security*, si sviluppa secondo un delicato equilibrio tra tutela dell'individuo e l'intervento di poteri (pubblici e/o privati) con una potenziale compressione delle libertà costituzionalmente garantite. Il recente fiorire dell'attenzione intorno al "costituzionalismo digitale" [13], una locuzione discussa e discutibile ma ormai invalsa nell'odierno dibattito, va inteso anche in questa direzione alla luce degli evidenti corollari in ordine al tema della cybersicurezza.

Di qui il terzo profilo poc'anzi segnalato: il reticolo normativo connesso alla cybersicurezza.

Non è luogo qui per ricordare tutto il complesso, nonché ancora in via di definizione, percorso di regolazione. Come noto, esso ha interessato sia la produzione normativa nazionale sia il livello sovranazionale laddove, almeno per ora e forse non a caso, minore è stata l'attenzione destatasi a livello di diritto internazionale. Senza ambire ad una rassegna esaustiva, occorre ricordare almeno il D.P.C.M 2013, la Direttiva europea 2016 NIS, il perimetro di sicurezza nazionale predisposto nel 2019 così come l'istituzione di una *authority* europea e nazionale nel 2021 (quest'ultime dotate di uno *status* giuridico un poco peculiare rispetto alle altre *authorities*)[14].

Sul punto ci si limita a formulare due rilievi tra loro connessi.

In primo luogo, occorre rimarcare la complessità di tale scenario.

Canada, Stati Uniti, Regno Unito (che all'epoca era ancora all'interno dell'Unione europea), Australia, Nuova Zelanda, Francia e Germania sono in grado di nuotare nella piscina dedicata agli adulti, gli altri Paesi devono accontentarsi della piscina dei bambini. La crisi ucraina ha messo in evidenza quanto la «teoria delle due piscine» fosse errata, perché mentre nel caso di una guerra tradizionale un'alleanza è forte quanto il suo membro più forte, in una guerra cibernetica un'alleanza è debole quanto il suo membro più debole. Ben presto l'Occidente ha compreso che per difendersi ha bisogno che tutti i sui membri siano affidabili e sappiano «nuotare» nelle piscine per adulti. Cosicché l'Europa per superare questa «teoria delle due piscine» ha puntato sulla conoscenza collaborativa, che è diventata la priorità fondamentale della cybersicurezza: tutti i soggetti che lavorano alla cybersicurezza di ciascuno Stato membro devono collaborare per condividere le informazioni. Si trattava di un passaggio delicato perché nei diversi stati la cybersicurezza è appannaggio di soggetti differenti, non sempre fra loro omogenei e compatibili, come ad esempio i servizi segreti, aggregazioni pubblico-privati, ecc.".

13 In merito ad esempio, da prospettive diverse, Dimasi 2023; Frosini 2021; Iannotti Della Valle 2023.

14 Oltre ai riferimenti contenuti nei testi citati nelle note precedenti e a quelli che verranno menzionati successivamente, su questi temi si rinvia innanzitutto, in modo un poco rapsodico, ad alcuni contributi di Indra Macrì (consigliere dell'area informatica della Corte Costituzionale): Macrì 2024, 2023, 2022a, 2022b, 2021. Inoltre, da una prospettiva essenzialmente amministrativistica, Golisano 2022; Parona 2021: 709-719; Renzi 2021: 538-548. In tema anche "Igiene e sicurezza del lavoro", 2, 2024, inserto dal titolo *Dalla direttiva ala regolamento sulle macchine; che cosa cambia? (Parte II)*, pp. III-XXIII.

Come già sottolineato, esso appare particolarmente intricato nonché, in qualche misura, contraddittorio e talora ridondante. Al suo interno si può intravedere la conferma di un profilo che, per vie diverse, la teoria del diritto va segnalando da tempo[15]: la crescente difficoltà di mantenersi entro i confini di una concettualizzazione assiomatica del normativo, quale quella originatasi in alcuni passaggi del Novecento e, a sua volta, radicata in un modello epistemologico di matrice ottocentesca a lungo reputato scientificamente saldo e operativamente fruibile[16]. Per questa via, si aprono gli spazi teorici per cogliere la rilevanza assunta progressivamente dai modelli giusreticolari[17], di cui la normativa concernente la cybersicurezza sembra costituire un ottimo esempio e sui quali si tornerà più avanti.

Ma l'ambiente normativo di cui si va ragionando contribuisce, altresì, alla ridiscussione dell'apparato dogmatico nel suo complesso. Più precisamente, in gioco sono le condizioni stesse alle quali la modernità giuridica (quantomeno a partire da Hobbes) era andata strutturandosi, anche in ordine alla configurazione del nesso certezza-sicurezza: profilo su cui ora occorre soffermarsi più compiutamente volgendo lo sguardo ai contesti contemporanei.

4. Cybersicurezza, AI e dogmatica giuridica

Su questo sfondo si può situare utilmente un carotaggio intorno al nesso tra cybersicurezza e intelligenza artificiale. In merito, si è giustamente osservato come si debba parlare di "rapporto di presupposizione tra i due plessi normativi, atteso che la cybersicurezza rappresenta una premessa indefettibile per un impegno sicuro dell'intelligenza artificiale", nel senso che "la prima [costituisce], dal punto di vista del diritto positivo, una componente necessaria del quadro normativo in cui la seconda possa essere sviluppata e utilizzata"[18].

Ad uno sguardo più ravvicinato, il tema cruciale è rappresentato dal posizionamento dell'intervento normativo qui inteso in termini articolati e, cioè, inclusivo del profilo cognitivo che accompagna strutturalmente il momento giuridico.

Un buon *test* per sviluppare, in controluce, tale riflessione è rappresentato dal regolamento europeo sull'intelligenza artificiale (d'ora in poi AI Act) che, come noto, va collocato nell'ottica di transizione digitale da tempo predisposta dall'Unione Europea e a sua volta da intendersi *pour cause* nel quadro di un forte nesso con la dimensione della sicurezza.

15 Mi permetto di rinviare a Bombelli 2017, in particolare capp. 3-4.

16 Si pensi, in modo paradigmatico, al nitore che connota una certa stagione del pensiero di Kelsen legata alla prima metà del secolo scorso e, in particolare, alla parabola teorica che, dalla sua *Reine Rechtslehre. Einleitung in die rechtswissenschaftliche Problematik.* Franz Deuticke, Wien, 1934, arriva sino alla nota riedizione di tale opera nel 1960.

17 Bombelli 2017, cap. 3.

18 Parona 2021: 711. Nell'ormai estesissima bibliografia dedicata all'intelligenza artificiale segnalo, per la ricchezza e varietà di spunti ivi proposti, D'Aloia 2020.

Senza ambire ad un'analisi esaustiva della normativa europea, a mo' di *focus* si propongono solo alcune notazioni con riguardo a taluni suoi aspetti o criticità.

Da una prospettiva di carattere generale, un primo profilo attiene alla novità, di portata non assoluta ma certamente rilevante, che connota lo strumento normativo di derivazione sovranazionale. Come noto, esso rappresenta a livello mondiale una delle prime forme di regolazione del fenomeno dell'intelligenza artificiale: più precisamente, l'AI Act può leggersi come l'esito di un bilanciamento tra scelte politiche, operate appunto a livello sovranazionale, e diritto. Un versante, quello del rapporto tra politica e diritto, che in proiezione appare decisivo anche in ordine al problema della sicurezza in chiave di cybersicurezza[19].

In secondo luogo, sempre ad un livello generale, nel documento europeo si staglia con chiarezza la problematicità del nesso tra tecnica e diritto. *Sub specie* della disciplina concernente l'intelligenza artificiale, si delinea la questione del rapporto tra mutamenti sociali e intervento normativo: più precisamente, lo scarto che intercorre tra la rapidità che vieppiù connota i primi e il "ritardo" nella plasmazione delle categorie giuridiche, con riflessi rilevanti sul piano della metodologia giuridica (sul punto si tornerà meglio più avanti).

Entrando più direttamente nella previsione normativa confezionata dal legislatore europeo, è possibile rimarcare alcuni aspetti specifici.

Innanzitutto, l'AI Act non intende regolamentare i "prodotti" legati all'intelligenza artificiale, bensì i suoi modelli o tipologie (i "processi") di natura "generativa". L'obiettivo è disciplinare le forme di intelligenza artificiale a *general purpose* che, come tali, si ritiene possano comportare un rischio sistemico[20].

Di qui l'impianto tecnico-normativo articolato e complesso[21].

Tra i molti aspetti che lo connotano, sempre con riguardo all'intelligenza generativa, in particolare vale la pena mettere in luce come nel documento europeo si individuino livelli differenti di rischio.

Da un lato, infatti, emerge il modello generativo ad alto rischio (o rischio sistemico). Esso richiede un aggiornamento *in progress* dei coefficienti, con i relativi oneri o adempimenti di carattere formale (avviso alle autorità competenti, trasparenza dei processi adottati, ecc. con i relativi dubbi concernenti la moltiplicazione dei soggetti predisposti alla regolazione).

Dall'altro, si pone l'intelligenza artificiale generale o "di base", comunque ritenuta non ad alto rischio. Riguardo ad essa, permane l'obbligo di trasparenza

19 Si veda *supra* nota 12.

20 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio (13 giugno 2024), nn. 84-85 (testo disponibile al https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689).

21 Si segnalano qui solo alcuni tratti che connotano il testo europeo: il lungo elenco iniziale di "considerando"; l'adozione di una certa forma linguistica o lessico; il rinvio a *authorities*; la presenza di norme programmatiche; l'apparato sanzionatorio (analogamente a quanto avviene nel GDPR); la definizione di IA proposta all'art. 3 (e allegato 1); l'esclusione dell'ambito militare; il *risk-based approach* su cui si tornerà poco più avanti.

circa il suo funzionamento, le modalità della sua creazione e la precisazione delle relative caratteristiche tecniche[22].

Tale modello complessivo presenta alcune criticità rilevanti anche in tema di *cybersecurity*.

La prima attiene alle tipologie di intelligenza artificiale. La distinzione tra intelligenza "generativa" e non "generativa" muove dal presupposto che essa permanga nel tempo: ciò a fronte di un processo di innovazione tecnologica sempre più rapido, che rischia di rendere tale distinzione rapidamente obsoleta.

Una seconda criticità attiene al concetto di "rischio". Il documento europeo propone la scansione tra rischio "inaccettabile" (con conseguente divieto), "alto"[23] e "basso" (o minimo). Si tratta di un *risk-based approach* già adottato in altre sedi che, tuttavia, forse omette di ragionare più a fondo sulla distinzione (giuridica) tra "rischio" e "pericolo": se il primo, in un'accezione per così dire tradizionale, appare sempre giuridicamente "calcolabile" o dominabile[24], va osservato che la graduazione della nozione di rischio risente delle incertezze epistemico-cognitive relative al fenomeno *de quo* e alla sua eventuale evoluzione di cui si è detto poc'anzi[25].

Anche le finalità che animano l'AI Act appaiono discutibili. A ben vedere, come peraltro accade di frequente in tema di normativa europea, sembra darsi una tensione tra due dimensioni. Da un lato si staglia la tutela dei diritti fondamentali richiamata nel preambolo e, al contempo, emerge l'attenzione rivolta al mercato: un profilo decisivo, ove si consideri il massiccio (e crescente) volume economico connesso al fenomeno dell'intelligenza artificiale e, conseguentemente, della cybersicurezza come dimensione ad essa connessa[26].

Di qui il tratto oscillante della disciplina in oggetto, con riguardo sia alla sua natura giuridica sia alla struttura complessiva. Si spiegano, così, alcune letture che di essa sono state offerte in termini di normativa "evolutiva" o, al contrario, "regressiva"[27], così come l'equilibrio problematico ivi disegnato tra "innovazione" e "diritti". Un profilo, quest'ultimo, che a ben vedere sembra connotare il quadro complessivo degli obiettivi generali perseguiti dall'Unione Europea, ad esempio a

22 Per i modelli di intelligenza artificiale di uso generale, o comunque non generativa (al *considerando* n. 97), valgono invece altre condizioni: la figura della "licenza", la presenza dell'*open source*, il ricorso a modelli e parametri resi pubblici.

23 Allegato 3 del regolamento europeo di cui si va ragionando.

24 Su questi temi si consenta rinviare a Bombelli 2022a: 177-230, in particolare 200 e ss.

25 Da questa prospettiva riemergono, in altro contesto, alcune istanze sottese all'ormai classico Beck 1986.

26 Nel capo I del Regolamento (UE) 2024/1689, dedicato alle *Disposizioni generali*, l'art. 1, comma 1 recita: "Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione".

27 Oscillazioni che si possono leggere anche in rapporto al contenuto e alle letture offerte di un documento normativo, come il regolamento Digital Markets Act (DMA) approvato dal Parlamento europeo del 5 luglio 2022, per molti versi connesso ai temi di cui si va ragionando.

partire dalla problematica tenuta (sul piano logico e operativo) del nesso operante tra transizione digitale e *green transition*: obiettivo, come noto, al cuore degli obiettivi del programma *Next Generation*[28] e presente anche nella disciplina relativa all'intelligenza artificiale.

Questi rilievi sembrano trovare conferma anche ad un altro livello e, cioè, con riguardo al *range* della normativa europea, la quale per definizione attiene all'ambito dell'Unione (a prescindere da alcuni casi delimitati[29]).

Il punto-chiave è rappresentato dalla natura trasversale dell'intelligenza artificiale: più estesamente, esso rinvia alla capacità strutturale dei mutamenti tecnologici di travalicare gli steccati statuali e sovranazionali. Detto in altri termini: viene qui a tema il problema del nesso tra spazio (o spazialità) e normatività, con evidenti riflessi in tema di cybersicurezza, come luogo classico di definizione del *nomos* e che, almeno a partire da Hobbes, non a caso rimonta alle origini della modernità dispiegandosi sino al dibattito contemporaneo (ad esempio in Carl Schmitt[30]) e alla problematicità della nozione stessa di "cyberspazio"[31].

Riguardato da una prospettiva più generale, il *case study* relativo all'intelligenza artificiale (e, per contiguità logica e tecnologica, alla cybersicurezza) consente di mettere in luce un preciso profilo teorico-giuridico.

Esso attiene alla natura, per così dire, reattiva assunta progressivamente dal diritto (a ben vedere anche in termini di *active defence*[32]): in altre parole, l'intervento

28 Nel senso che un profilo talora può configgere con l'altro: come noto, ove realmente e globalmente perseguita la transizione digitale presenta una serie di costi (economici, sociali e soprattutto ambientali) tale da rendere altamente problematico ambire al contempo, in modo praticabile e realistico, ad una *green transition*.

29 Ça va sans dire si versa in tema di disciplina direttamente applicabile negli Stati membri dell'Unione europea. Per le ipotesi di estensione della normativa al di fuori di tale orizzonte e, più ingenerale, per il rapporto tra quadro comunitario e spazio giuridico ad esso esterno, rinvio a quanto espressamente contemplato nel regolamento europeo relativo all'intelligenza artificiale (ad esempio il *considerando* 46).

30 Si rinvia *supra* n. 3.

31 Nel Regolamento europeo relativo all'intelligenza artificiale la nozione di "spazio", in particolare secondo la dizione "spazio normativo", ricorre frequentemente nei *Considerando* e in altri luoghi: tuttavia, come segnalato *supra* alla n. 9, a livello di strategia europea la saldatura tra il tema della *cybersecurity* e la concettualizzazione della categoria di *cyberspazio* in termini di dimensione "aperta e sicura" risale al 2013. Più in generale, circa il nesso spazio-normatività nell'orizzonte tecnologico si consenta rinviare Bombelli 2010, in particolare cap. 5: 483 e ss.

32 Con riguardo specifico alla cybersicurezza, ciò si evince dal problema della proprietà dei modelli e dei sistemi, ove la regolazione giuridica avviene "a valle", senza intaccare l'originaria disponibilità del "bene" e della sua strutturazione a livello tecnologico in capo al produttore inteso come soggetto privato. Per spunti in tal senso Renzi 2021: 538-539: "La consapevolezza dei pericoli connessi a [fenomeni di attacco cibernetico] ha portato il legislatore a sostituire un approccio di mero contrasto occasionale e la repressione criminale dei comportamenti, con una strategia normativa in grado di assicurare la sicurezza cibernetica preventiva, limitando le possibilità di attacco e riducendo gli eventuali danni che possono essere subiti. L'assunto risulta ancor più vero nel settore che per eccellenza richiede interventi preventivi, quale appunto quello della sicurezza nazionale. Basti pensare, sul punto, a come gli approfondimenti del *World Economic Forum* equiparino gli attacchi informatici alle grandi crisi economico-finanziarie in termini di capacità di influenza sulla stabilità e sulla sicurezza internazionale" (p. 538). Ivi si veda inoltre

normativo sembra situarsi sempre più "a valle" del mutamento tecnologico, assumendo in tal senso una sorta di ruolo ancillare[33]. Ne discende un fenomeno per molti versi nuovo che interessa la relazione tra due dimensioni: l'edificazione della dogmatica giuridica e l'emergere del "fatto sociale (*rectius* tecnologico)".

Se il diritto moderno, con il relativo corredo storico-categoriale, era andato caratterizzandosi per la capacità in qualche modo di pianificare *ex ante* (se non "guidare") il *novum* sociale garantendo la certezza dell'intervento normativo e l'ideale della sicurezza, ciò cui si assiste è una sorta di rovesciamento delle parti.

Ne consegue che la costruzione delle categorie giuridiche, intese propriamente come griglie di lettura dei fenomeni sociali, sembra plasmarsi esclusivamente in funzione di processi in qualche modo *già* compiuti e definiti, nonché alla luce di dimensioni (come in particolare la tecnologia e l'economia) in grado di elaborare autonomamente modelli "interni" di razionalità e che la sfera giuridica si limita a mutuare[34]. Un quadro problematico e categoriale che, nel suo insieme, sembra attestare la transizione progressiva da un repertorio teorico di derivazione moderna a un orizzonte vieppiù abitato da contesti e categorie ad essa eterogenee: riprenderemo il punto in conclusione.

Occorre allora rimeditare il circuito concettuale imperniato sul binomio dogmatica giuridica-certezza del diritto, una sorta di roccaforte teorica della modernità, ove soprattutto si intenda il secondo termine del binomio in termini di calcolabilità (e progressiva in-calcolabilità delle dinamiche *in fieri*) nell'accezione precisata precedentemente, anche alla luce dei profili cognitivi sottesi a tali nuclei concettuali: su questo si concentrerà l'attenzione nelle seguenti pagine conclusive.

5. Per concludere: "anticipazione cognitiva", *legal design* e *decision-making*

La riflessione proposta nelle pagine precedenti apre ad una serie di proiezioni che investono sia il tema della sicurezza (anche nella prospettiva specifica della *cybersicurezza*) sia, in chiave più generale, l'orizzonte teorico e socio-giuridico entro il quale essa sin da ora va modulandosi.

(pp. 546-547) la comparazione con altri assetti normativi (in particolare USA, Grecia, Francia), con la seguente conclusione: "Le vere sfide che caratterizzeranno il prossimo futuro […] saranno connesse […] alla capacità del *framework* [normativo] di assicurare un ampio livello di collaborazione europea, ma anche interistituzionale e con gli operatori privati. Questi ultimi, infatti, oltre a poter fornire un ampio *know know* e a configurarsi come i principali innovatori nel settore, richiedono una costante attività di supporto da parte delle istituzioni. Proprio l'Agenzia nazionale, nonostante il suo non chiaro posizionamento nel contesto del Sistema di informazione nazionale, può porsi come l'interlocutore privilegiato per il superamento di un'ottica di mera vigilanza e controllo, verso una dimensione più partecipata e collaborativa. Questo sulla base proprio della costante interconnessione tra reti ed infrastrutture digitali, che molto speso provoca una sostanziale riduzione delle differenze tra pubblico e privato".

33 Per un quadro più ampio Bombelli, Montanari 2015.

34 In merito mi permetto di rinviare a Bombelli 2015b: 321-358. Profili problematici sono variamente presenti anche in Bombelli 2015a e in Bombelli, Lavazza 2019: 3-34.

Uno scenario, va da sé, articolato e complesso di cui in questa sede si è provato a segnalare almeno alcuni tratti distintivi. Muovendo dal quadro proposto, a mo' di conclusione di seguito si ritagliano tre rilievi che, da un orizzonte generale di natura teorico-giuridica, investono le nozioni di *legal design* e *decision-making* e la cui sequenzialità concettuale apre ad un interrogativo finale.

Il primo versante attiene alle proiezioni in tema di teoria del diritto.

L'esigenza poc'anzi rimarcata di ripensare il nesso tra dogmatica e certezza postula simmetricamente, in chiave più ampia, l'esigenza di rivedere i momenti strutturali che connotano l'intervento normativo, nonché gli schemi concettuali attraverso i quali il diritto legge la realtà sociale e, a sua volta, si autocomprende. L'analisi proposta mostra come appaia ormai quantomeno tortuoso il ricorso a modelli di *geometria juris* di ascendenza moderna o, analogamente, il rinvio a paradigmi *lato sensu* logico-assiomatici di "scienza del diritto" **à la** Kelsen maturati tra fine Ottocento e prima metà del secolo scorso.

Beninteso, ciò non significa abdicare alle istanze sottese alla modernità giuridica. Al contrario: l'esigenza di preservare il "cuore" del moderno giuridico, assiso sul binomio più volte evocato di dogmatica e certezza come sicurezza "calcolabile" con le correlate tutele della sfera soggettiva, richiede di misurarsi apertamente con paradigmi teorico-giuridici inediti.

Ed è qui che si stagliano i modelli reticolari cui si è accennato in precedenza. Prodottisi a seguito di una sorta di circolare rispecchiamento tra prassi e teoria, essi risultano funzionali a comprendere le dinamiche di cui si va ragionando costituendone, in parte, l'esito a livello teorico[35].

Un buon esempio è rappresentato proprio dall'assetto normativo concernente la cybersicurezza e, in combinato disposto, almeno in parte anche dalla disciplina relativa all'intelligenza artificiale. Il crescente articolarsi di disposizioni, così come il fiorire di *authorities* nazionali e sovranazionali dallo *status* ibrido[36], comporta un intersecarsi e parziale sovrapporsi di modelli di regolazione ad andamento reticolare: riflessivamente ne consegue il radicarsi di una autolettura "a rete" della sfera giuridica, con il conseguente incrinarsi del binomio moderno rappresentato dalla dimensione dogmatica e dal binomio certezza-sicurezza.

Di qui l'esigenza di rimarcare il ruolo della dimensione cognitiva sottesa ai nodi problematici sin qui segnalati. Intesa come dotazione epistemica[37], *ça va sans dire*

35 Bombelli 2017, in particolare cap. 3 circa il significativo fenomeno di rispecchiamento tra teoria e prassi e l'originarsi di un modello teorico inedito.

36 Parona 2021: rimarcando la molteplicità di ambiti investiti dalla *cybersecurity* e l'intersecarsi del livello privato e pubblico, l'Autore enfatizza la natura composita e in divenire della relativa disciplina (europea e nazionale). Si vedano, in particolare, le pp. 714-719 circa l'ambiguità e ibridità dell'*authority* nazionale, nonché la sua collocazione (in quanto disciplina *ad hoc*) nel quadro dell'articolazione dei poteri, con rilievi in ordine alla natura *command and control* di tali enti regolativi anche in relazione al crescente nesso tra *cybersecurity* e intelligenza artificiale.

37 La categoria o nozione di "cognitivo" è strutturalmente complessa: per un possibile sondaggio teorico Bombelli 2022b: 71-97. Le matrici originarie di tale prospettiva sono già presenti in Bombelli 2017, in particolare l'Introduzione e i capp. 1-2 con riguardo alla crucialità rivestita dall'orizzonte del "senso comune" (*common sense*) nel costituirsi dell'esperienza giuridica.

essa rappresenta da sempre una *conditio sine qua non* del diritto: da questa prospettiva, i temi di cui si va ragionando costituiscono una sorta di laboratorio del tutto peculiare. A ben vedere, la natura per molti versi "in-calcolabile" dei processi ascrivibili alla cybersicurezza richiede un *surplus* di dotazione cognitiva sia sul piano teorico, sia nella prassi di tutti gli operatori giuridici.

In tal senso appare allora plausibile parlare di "anticipazione cognitiva".

Più precisamente, con essa si fa riferimento all'esigenza di (ri)anteporre l'intervento normativo, colto appunto nella sua dimensione anche cognitiva, al *datum* sociologico (*rectius*: al fenomeno tecnologico) intervenendo "a monte" del medesimo. Per questa via, si tratta di ripristinare lo schema teorico maturato nella modernità e in cui, come osservato, al diritto si attribuiva propriamente il ruolo di griglia concettuale in grado di articolare, mediante le sue categorie, i fenomeni sociali.

Le proiezioni di tale prospettiva si possono cogliere distintamente in ordine a due figure tra loro connesse: il *legal design* e i processi di *decision-making*.

L'espressione *legal design*[38] viene qui utilizzata in termini semanticamente estesi.

Con essa si fa riferimento non solo al significato ordinario che, come noto, attiene alle modalità di redazione della disciplina giuridica tese a garantirne chiarezza, trasparenza e fruibilità, ma anche alla capacità della previsione normativa di cogliere il *proprium* del fenomeno regolato (in tal caso di natura tecnologica).

In altre parole, il *focus* va sull'insieme dei processi sottesi alla plasmazione quanto più pertinente dell'intervento giuridico. Si pensi, ad esempio, alla struttura degli algoritmi: il punto è diradarne l'intrinseca opacità, soprattutto a livello di valutazione giuridica, creando le condizioni affinché il diritto possa entrare "a monte" nei meccanismi cognitivi e *quindi* normativi che presiedono alla loro elaborazione.

Un versante, del resto, ben noto al diritto come avviene in ordine alla concettualizzazione di alcune nozioni, quali quelle già evocate, di "rischio" o di "principio di precauzione".

In esse la disciplina giuridica si configura necessariamente alla luce di una valutazione anche e soprattutto di tipo cognitivo, con riguardo alla specifica struttura delle materie regolate[39]. Da questa prospettiva, è il grado di *cognitum* a determinare l'*an* e il *quomodo* dell'intervento normativo: uno schema concettuale che, ad esempio, dal *climate change* si può estendere all'orizzonte della cybersicurezza, ove soprattutto ove si consideri quest'ultima in continuità logica con l'intelligenza artificiale.

Profili che si riflettono inevitabilmente a livello di configurazione del *decision-making*.

Analogamente a quanto poc'anzi osservato con riguardo alla nozione di *legal design*, anche in tal caso tale espressione va colta nella sua più ampia estensione. Con tutta evidenza essa investe immediatamente le forme del binomio sfera privata-sfera pubblica, ove in ultima istanza quest'ultima coincide con la dimensione politico-istituzionale *tout court*: ciò che rinvia al *continuum* 'sicurezza-funzionalità della democrazia'.

38 Per una presentazione agile e sintetica De Muro, Imperiale 2021.

39 Su queste nozioni rinvio a Bombelli 2022a (vedi anche *supra*).

Di qui, in termini più generali, l'esigenza di ripensare radicalmente il nesso tra meccanismi di produzione del sapere, diffusione della conoscenza e forme di regolazione del vivere associato.

Sotto questo profilo, come qualcuno suggerisce da tempo, acquista allora maggiore plausibilità l'apertura ad una sorta di "coproduzione" tra sapere scientifico (inclusivo delle sue più recenti proiezioni tecnologiche) e diritto[40]. A ben vedere, nell'idea di "co-produzione" si sintetizzano i profili epistemico-cognitivi e regolativi più volte evocati e che, come osservato, l'orizzonte della sicurezza (*sub specie* della cybersicurezza colta come spazio e luogo di esercizio di un potere di natura pubblica) enfatizza in modo peculiare. In definitiva, si tratta di creare le condizioni funzionali a un modello di intervento normativo "cognitivamente maturo" così da attingere, al contempo, a un gradiente di maggiore "democraticità" del sapere.

Ne discende un circuito logico. L'eventuale rimeditazione delle dinamiche di *decision-making* e delle relative *policies* rifluisce sulla configurazione del binomio pubblico-privato, nel quadro di uno scenario fortemente cangiante e in cui il tema della cybersicurezza riveste un ruolo potenzialmente decisivo[41].

Con uno sguardo d'insieme, si tratta di uno scenario connotato da prospettive problematiche e internamente complesse. Esso sembra confermare, come inizialmente accennato, la transizione progressiva dal paradigma moderno ad una grammatica concettuale differente, in grado di mettere in discussione i luoghi teorici decisivi intorno ai quali il primo era andato strutturandosi.

Ciò emerge con particolare riguardo alla sequenza, che di seguito si può solo sinteticamente tratteggiare, disegnata dalle nozioni di "spazio", "soggetti istituzionali", "fonti giuridiche", "norma" e, infine, dalla polarità "pubblico-privato" con la conseguente proiezione sui modelli statuali.

L'intrinseca problematicità del profilo regolativo (nazionale, sovranazionale e, ove presente, internazionale) quale emerge paradigmaticamente in tema di *cybersecurity* attesta, più in generale, la pervasività della tecnologia compromettendo la coppia concettuale di matrice moderna e statuale legata al nesso spazio-norma a base territoriale.

A cascata, muta anche il repertorio dei soggetti istituzionali. La rassicurante individuazione delle competenze risalente alle origini della modernità appare progressivamente inidonea a governare fenomeni strutturalmente refrattari a delimitazioni normative troppo nette, in tal modo originando una moltiplicazione degli attori normativi (come avviene paradigmaticamente con le *authorities*).

Ciò si riverbera sulla galleria delle "fonti" e, più estesamente, sull'idea di "ordinamento".

40 Intorno alla tesi della coproduzione tra conoscenza scientifica e diritto ragiona da tempo Mariachiara Tallacchini: una sintesi preziosa in Tallacchini 2012: 313-336.

41 Si fa qui riferimento a fenomeni molteplici ed eterogenei, come l'emergere di sistemi privati di cybersicurezza o a forme di partenariato pubblico-privato connesso all'istituzione di un polo strategico nazionale. In merito, ad esempio, Renzi 2021: 44.

L'implementarsi di normative a struttura reticolare, attraverso il crescente ricorso ad una disciplina dei fenomeni secondo uno schema a "cloud"[42], non solo revoca in dubbio la categoria stessa di "fonte" ma compromette, altresì, i modelli teorico-giuridici di natura sistematico-ordinamentale variamente elaborati nella tradizione precedente.

Simmetricamente cambiano gli schemi di lettura della "norma" giuridica. Sotto questo profilo, anche il binomio ormai risalente *hard law-soft law* appare in qualche modo logoro e insoddisfacente: a ben vedere, l'intero plesso regolativo dell'universo digitale, a partire dalle norme europee, si connota per una strutturale fluidità tipologica e concettuale.

Per questa via, infine, in prospettiva la riconfigurazione del binomio privato-pubblico[43] più volte rimarcata sembra postulare uno spazio *lato sensu* "pubblico" sinergicamente regolato da attori molteplici (al contempo "privati" e "pubblici" nell'accezione tradizionale). In tale riconfigurazione, inoltre, si intravede *in nuce* la trasformazione progressiva (reale o potenziale) del senso e del ruolo rivestito dalla "sicurezza" come orizzonte della narrazione giuridica moderna.

All'interno del modello delle fonti, definibile a "geometria varabile" e strutturalmente *in progress*, i fenomeni legati al tema della cybersicurezza mostrano, infatti, come l'obiettivo tuzioristico perseguito dal moderno possa realmente trasformarsi nel suo opposto interessando il complessivo assetto statuale. Più precisamente, ciò che viene a tema è la relazione tra Stato (come luogo "classico" del potere) e tecnologia (configurata come *cybersecurity*), con la sua eventuale declinazione in chiave tecnocratica.

Si tratta, allora, di ragionare non solo in termini di "sicurezza *del* potere" ma anche in chiave di "sicurezza *dal* potere"[44]: con lessico hobbesiano, il punto è la prevalenza progressiva della *security* sulla *safety*. La questione della trasparenza della *cybersecurity*, strumento di tutela della sfera individuale e al contempo potenziale forma controllo della medesima, si salda così all'ormai noto problema dei *Big data* in vista della plasmazione di una *governance* complessiva dei processi di cui si va ragionando. Sullo sfondo si intravede il possibile stagliarsi, forse in modo non troppo paradossale, della (cybers)sicurezza come una sorta di panottico digitale, originando una silente microfisica del potere[45] segnata dalla latente torsione del modello liberale in chiave di paternalismo democratico-tecnologico.

42 Ove la nozione di "cloud" non rinvia solo all'oggetto regolato, riferendosi essa anche ad alcuni profili della relativa tecnica regolativa. In merito, ad esempio, Macrì 2023 (con riguardo alle modifiche intervenute nel luglio 2023) e Macrì 2024; inoltre Macrì 2022b.

43 In merito si veda anche la recente presa di posizione di Unione Europea e dei suoi Stati membri in ordine alla nozione di "cyberspazio" finalizzata all'implementazione di modelli di cybersecurity: https://www.cybersecurity360.it/news/diritto-internazionale-nel-cyberspazio-ecco-le-regole-ue-per-la-corretta-applicazione/.

44 Sul punto si consenta rinviare nuovamente a Bombelli 2015a, in particolare: 70 e ss. (in particolare: 75-86, con riguardo sia ai riflessi giuridici in chiave teorica e operativa, sia al nesso tra antropologia e modello liberale).

45 Con ovvio riferimento al classico Foucault 1977.

Sono queste le ragioni che spingono a rimarcare il ruolo decisivo rivestito dalla dotazione cognitiva quando si ragiona del "diritto dell'era digitale"[46]. A ben vedere, il riferimento al momento cognitivo rileva non solo sul piano dell'ideazione del *framework* regolativo dei fenomeni tecnologici ma, in senso più ampio, come *conditio sine qua non* del corretto funzionamento degli apparati democratici (come ribadito espressamente, ad esempio, anche all'art. 1 del Regolamento sull'intelligenza artificiale evocato nelle pagine precedenti)[47].

Questioni e istanze che, come segnalato, aprono a un interrogativo conclusivo nel quale si può condensare l'itinerario teorico sin qui proposto dischiudendo orizzonti da decifrare.

Ove si intenda la sicurezza come un tratto (se non la *cifra*) della modernità giuridica, al contempo enfatizzando il nesso politica-diritto sotteso alla declinazione specifica del tema sicuritario moderno rappresentata dalla cybersicurezza, l'eventuale sottovalutazione dei profili cognitivi può comportare la delegittimazione dei sistemi democratici?

Un plesso tematico da dissodare e in attesa di risposte teoriche e operative.

Bibliografia

Beck U. 1986, *Risikogesellschaft Auf dem Weg in eine andere Moderne*, Frankfrut am Main: Suhrkamp.

Bombelli G. 2022a, "Causalità e diritto: paradigmi e alcune questioni teoriche, in *Jus*, 1-2: 177-230.

Bombelli G. 2022b, "Cognitive Turn? Tra giuspositivismo e giuscognitivismo. Alcuni riflessi socio-giuridici", in *Sociologia del diritto*, 1: 71-97.

Bombelli G. 2018, "Segno, simbolo, diritto: tra semiotica e semantica. Argomenti per un'ipotesi di lavoro", in Manzin M., Puppo F., Tomasi S. (a cura di), *Studies on Argumentation & Legal Philosophy / 3Multimodal Argumentation, Pluralism and Images in Law*, Trento: Università degli Studi di Trento: 5 ss.

Bombelli G. 2017, *Diritto, comportamenti e forme di "credenza"*, Torino: Giappichelli.

Bombelli G. 2015a, "Circuiti pericolosi: la sicurezza tra potere, mercato e contesti postmoderni", in F. Pizzolato-P. Costa (a cura di), *Sicurezza, Stato e mercato*, Milano: Giuffré: 47 ss.

Bombelli G. 2015b, "Diritto, decisione e paradigmi di "razionalità", in Bombelli G., Montanari B. (a cura di), *Ragionare per decidere*, Torino: Giappichelli: 321-358.

Bombelli G. 2010, *Occidente e 'figure' comunitarie. Volume introduttivo: "Comunitarismo" e "comunità". Un percorso critico-esplorativo tra filosofia e diritto*, Napoli: Jovene.

Bombelli G., Lavazza A. (a cura di) 2021, *Diritto e neuroscienze. Nuove prospettive*, Milano: Mimesis.

46 Mutuo l'espressione da Pascuzzi 2025: ivi si veda in particolare, per i temi discussi nel presente contributo, il cap. 26 *Cybersicurezza e rischio digitale*.

47 Ciò, soprattutto, ove si ponga mente al rapporto vieppiù ineludibile che il diritto intratterrà con altri saperi come, ad esempio, con l'ambito delle neuroscienze: in merito Bombelli, Lavazza 2019 e, più ampiamente, i saggi proposti in Bombelli, Lavazza 2021.

Bombelli G., Lavazza A. 2019, "Tecnologia, processi decisionali, sfera pubblica e diritto. Esplorazioni", in Buzzacchi C., Costa P., Pizzolato F. (a cura di), *Technopolis. La città sicura tra mediazione giuridica e profezia tecnologica*, Milano: Giuffré Francis Lefebvre: 3-34.
Bombelli G., Montanari B. (a cura di) 2015, *Ragionare per decidere*, Torino: Giappichelli.
Brighi R. 2021, "Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati", in Casadei T., Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano: Cedam: 135-147.
Buzzacchi C., Costa P., Pizzolato F. (a cura di) 2019, *Technopolis. La città sicura tra mediazione giuridica e profezia tecnologica*, Milano: Giuffré Francis Lefebvre.
Casadei T., Pietropaoli S. (a cura di) 2021, *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano: Cedam.
Cocco G. (a cura di) 2012, *I diversi volti della sicurezza*, Milano: Giuffré.
Cortesi A.D. (a cura di) 2019, *ICT e diritto nella società dell'informazione*, Torino: Giappichelli.
D'Aloia A. (a cura di) 2020, *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano: Franco Angeli.
De Muro B., Imperiale M. 2021, *Legal design*, Milano: Giuffrè, Milano.
Dimasi L. 2023, *I diritti ipermoderni: sfide e cambiamenti nell'era del costituzionalismo digitale*, Bologna: Bologna University Press.
Faini F., Pietropaoli S. 2021, *Scienza giuridica e tecnologie informatiche. Temi e problemi*, Torino: Giappichelli.
Foucault M. 1977, *Microfisica del potere*, Torino: Einaudi.
Frosini T.E. 2021, *Apocalittici e integrati. La dimensione costituzionale della società digitale*, Modena: Mucchi.
Galli G. 1995, *La politica e i maghi. Da Richelieu a Clinton*, Milano: Rizzoli.
Galli G. 1989, *Storia delle dottrine politiche*, Milano: Il Saggiatore.
Giaccardi C., Magatti C. 2022, *Supersocietà. Ha ancora senso scommettere sulla libertà?*, Bologna: il Mulino.
Giannuli A., Curioni A. 2019, *Cyberwar. La guerra prossima ventura,* Milano-Udine: Mimesis.
Golisano L. 2022, "Il governo del digitale: strutture di governo e innovazione digitale", in *Giornale di diritto amministrativo*, 6: 824-834.
Greco T. (a cura di) 2009, *Dimensioni della sicurezza*, Torino: Giappichelli.
Hobbes T. 2001 [1651], *Leviatano*, Parte I, XIV, 9-11, Milano: Bompiani.
Iannotti Della Valle A. 2023, *Le regole di Internet tra poteri pubblici e privati. Tutela dei diritti e ruolo dell'antitrust in una prospettiva costituzionale*, Napoli: Editoriale Scientifica.
Irti N. 2016, *Un diritto incalcolabile*, Torino: Giappichelli.
Macrì I. 2024, "Cybersicurezza, le novità per il 2024", in *Azienditalia*, 1: 17-22.
Macrì I. 2023, "Regolamentazione cloud: le novità per la PA", in *Azienditalia*, 11: 1334-1339.
Macrì I. 2022a, "Il PNNR italiano per la digitalizzazione della Pubblica Amministrazione", in *Azienditalia*, 1: 38-56.
Macrì I. 2022b, "Dalle infrastrutture digitali delle Amministrazioni al cloud, il nuovo regolamento per la sicurezza dei dati e dei servizi pubblici", in *Azienditalia*, 3: 488-504.
Macrì I. 2021, "Cybersicurezza per la Pubblica Amministrazione", in *Azienditalia*, 12: 1996-2006.
Pacchi A. 2004, *Introduzione a Hobbes*, Bari: Laterza.
Parona L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale di diritto amministrativo*", 6: 709-719.

Pascuzzi G. 2025, *Il diritto dell'era digitale*, Bologna: il Mulino.
Pizzolato F., Costa P. (a cura di) 2015, *Sicurezza, Stato e mercato*, Milano: Giuffré.
Renzi A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giornale di diritto amministrativo*, 4: 538-548.
Schmitt C. 1991 [1974], *Il Nomos della terra nel diritto internazionale dello 'jus publicum Europaeum'*, Milano: Adelphi.
Tallacchini M. 2012, "Scienza e diritto. Prospettive di co-produzione", in *Rivista di Filosofia del diritto*, 1 (2). 313-336.
Ziccardi G. 2022, *Diritti digitali. Informatica giuridica per le nuove professioni*, Milano: Cortina.

Elena Buoso

Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica

Abstract: L'evoluzione dei sistemi giuridici ha avuto un impatto significativo sulla funzione di sicurezza pubblica, ridefinendone i concetti e le pratiche. Le categorie tradizionali della teoria generale della sicurezza, come i principi di precauzione e prevenzione, e l'uso di concetti giuridici indeterminati per legittimare il potere esercitato, rivelano la complessità nel rispondere alle nuove sfide e la necessità di stabilire criteri per bilanciare il potere e gli interessi coinvolti. La sicurezza, considerata come un concetto olistico e multiforme, si è ampliata fino a includere la dimensione della cybersecurity, un'area sempre più centrale nelle moderne politiche di sicurezza, ampliando così anche il potere amministrativo per la protezione preventiva. Uno dei nuovi strumenti attraverso cui si esercita questa antica funzione è il Perimetro nazionale di sicurezza cibernetica. Esso rappresenta uno strumento cruciale per la tutela degli interessi strategici del Paese, individuando i soggetti ivi inclusi per imporre obblighi preventivi e successivi per la protezione delle funzioni e dei servizi essenziali dello Stato. La natura del potere esercitato in questo contesto, le peculiarità del procedimento amministrativo e gli effetti sull'attività dei soggetti inclusi sollevano importanti questioni relative alle garanzie e alle tutele necessarie a bilanciare la sicurezza nazionale con i diritti individuali e collettivi.

Keywords: Cybersecurity; Protezione preventiva; Perimetro di Sicurezza Nazionale Cibernetica; Procedimento amministrativo.

1. La funzione di pubblica sicurezza e l'evoluzione degli ordinamenti giuridici

Rischio, pericolo e, di conseguenza, paura, sono elementi che caratterizzano la percezione umana del mondo e influenzano l'azione individuale e collettiva. Già nel 1986 la migliore sociologia descriveva le peculiarità della nuova "società del rischio" e dei suoi percorsi verso una nuova modernità[1].

1 Beck 1986: 1. V. anche Luhmann 1991: 9; Bauman 2006: 54.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760158

Come sempre avviene, le conquiste tecnologiche degli ultimi decenni hanno portato anche nuove minacce e negli ultimi lustri gli ordinamenti giuridici registrano un aumento degli strumenti di protezione contro pericoli inediti, sviluppando strategie di difesa non solo in ottica nazionale ma anche, vista la dimensione e le caratteristiche dei fenomeni, globale[2]. Si tratta, peraltro, di fenomeni regolatori ricorrenti, con ricaduta su diversi istituti e branche del diritto, ai quali abbiamo assistito più volte nel corso del secolo scorso per reagire al terrorismo nazionale[3] e internazionale[4], alla criminalità organizzata[5], alla violenza negli e fuori dagli stadi[6].

La reazione degli ordinamenti, e in particolare di quello italiano, ha preso anche la strada del diritto amministrativo, con strumenti tradizionali o introducendo istituti nuovi, in un complesso di misure molto varie, dai controlli e dall'inasprimento di regimi autorizzatori o di divieti, alle *black list*, alle interdittive antimafia, ai d.a.s.p.o. Il panorama è molto ampio perché la funzione legata alla sicurezza è una delle funzioni primarie dell'apparato statale, infatti la troviamo descritta e analizzata diffusamente già dai primi trattati di diritto amministrativo[7].

Curiosamente, l'interesse della dottrina amministrativistica si è successivamente spostato su altri oggetti, un po' perché nella dialettica libertà e autorità è intervenuto il diritto costituzionale[8], ma anche perché altri settori sono risultati più rilevanti per il loro impatto economico e per un concetto di diritto amministrativo come fattore di sviluppo (si pensi agli appalti)[9]; o ancora perché l'attenzione si è rivolta alla cura di interessi differenziati e sensibili, come ambiente, paesaggio, sanità[10]. La funzione di pubblica sicurezza in sé, invece, non è stata particolarmente ulteriormente indagata con contributi di portata generale[11], se non per singoli aspetti che interferiscono con quel diritto amministrativo 'dell'economia'[12]. Il disinteresse

2 V. ad es., con riferimento al terrorismo, Haubrich 2003: 3-28; con riguardo alle minacce informatiche e alla cybersicurezza si segnalano i dati pubblicati dalle Nazioni Unite al sito https://unctad.org/page/cybercrime-legislation-worldwide nonché Kipker and Pagel 2020: 1 e le analisi comparate e nazionali pubblicate dalla Rivista International Cybersecurity Law Review – Zeitschrift für Cybersicherheit und Recht; Chiti 2016: 511.

3 Spataro 2023: 1-26.

4 Braml J. 2021: 2-26; Prosperi 2016: 16 e gli altri contributi del medesimo Volume.

5 Maggio 2013: 808; Passarelli 2024: 150-173.

6 D'Arienzo 2012: 1131; Follieri 2017: 23; Garaffa 2017: 399; Bifulco 2018: 159; Di Nella 2018: 77.

7 Orlando 1904: 71, la descrive come "quella funzione che tende a prevenire il danno sociale e ad assicurare la pace e l'ordine pubblico ed esercita una influenza sui diritti individuali, limitandone la sfera di azione in maniera che si mantenga l'armonia fra essi e fra l'utilità singola e quella collettiva"; v. anche Romano 1912: 244.

8 Mortati 1975: 135; Barile 1967: 12; Cerrina Feroni e Morbidelli 2008: 31; Matteucci 2016: 20; D'Atena 2018: 6.

9 Napolitano 2014: 695.

10 Sciullo 2016: 58.

11 Con alcune eccezioni: Corso 1979; Caia 2000: 184; Tropea 2010; e con un ritrovato interesse in tempi più recenti Tonoletti 2022: 791; Ursi 2022; Buoso 2023; Raimondi 2023.

12 Come il già richiamato istituto delle interdittive antimafia, sulle quali esiste una letteratura molto abbondante. V. ad es. Sticchi Damiani e Amarelli 2016: 11; Mazzamuto 2018: 2222.

è curioso[13], considerando non solo che ci si trova di fronte a una funzione squisitamente afferente al concetto di sovranità e di interesse pubblico[14] – e quindi al ruolo tradizionale dello Stato e della pubblica amministrazione – ma anche che essa implica poteri che incidono su diritti e libertà ed è quindi rivelatrice della concezione di Stato e di pubblica amministrazione del periodo storico di volta in volta considerato.

Sicurezza e prevenzione sono elementi ricorrenti, perché necessari al mantenimento del sistema e dell'ordinamento, ma con connotazioni e implicazioni molto differenti. Oggi sono lontane le teorie dell'individuazione dell'interesse pubblico e dei poteri autoritativi della pubblica amministrazione come garanzia totalizzante del benessere sociale[15] – che tra le Due Guerre hanno portato alle distorsioni dei regimi totalitari[16] – ma alcune suggestioni in questa direzione non sono assenti dagli atti legislativi in materia di pubblica sicurezza. In questo senso può essere letta anche l'attuale definizione degli scopi dell'Unione Europea in termini di creazione di "uno spazio di libertà, sicurezza e giustizia", che fonda e legittima la pervasività della regolazione unionale (art. 3, II c., TUE).

2. La teoria generale della sicurezza: prevenzione, precauzione e concetti giuridici indeterminati

Le considerazioni di teoria generale sulla funzione di sicurezza sono state recuperate in relazione al potere di prevenzione, impostosi con sempre maggiore evidenza come principio cardine dell'azione amministrativa – assieme al successivo principio di precauzione – in molti settori critici, quali il diritto dell'ambiente e della salute pubblica[17]. Entrambi i principi, infatti, sono riferiti a poteri limitativi della sfera giuridica dei privati, anticipatori rispetto all'evento e conformati da concetti giuridici indeterminati[18]. Nel caso dei poteri di sicurezza, i concetti giuridici indeterminati trovano la loro massima applicazione; essi infatti riguardano la *ratio* del potere (sicurezza, ordine pubblico e come abbiamo sentito ieri interessi nazionali strategici), l'individuazione dei presupposti dell'agire (rischio, pericolo) e la qualificazione dell'oggetto di esso (attività pericolose, servizi essenziali).

13 Sul disinteresse della scienza del diritto amministrativo per il tema, v. Cassese 2000: 127; Raimondi 2023: 2.

14 Fisichella 2008: 65.

15 Ranelletti 1904: 269, riprendendo le note tesi di O. Mayer.

16 Con riferimento allo Stato nazionalsocialista v. Schwegel 2005: 132; in relazione allo Stato fascista, cfr. Groppali 1940: 79; Panza 1990: 3; Cassese 2010: 14.

17 De Leonardis 2005: 6; Trimarchi 2005: 1673; Barone 2006; Manfredi 2011: 28. Esemplare in questo senso la giurisprudenza in materia di contrasto della Xylella fastidiosa nella vicenda che ha riguardato gli espianti degli ulivi in Puglia per contenere il fenomeno del disseccamento (Corte giustizia UE, sez. I, 9 giugno 2016, n. 78; Consiglio di Stato, sez. III, 11 marzo 2021, n. 2096) e quella relativa all'obbligo vaccinale previsto per alcune categorie di lavoratori durante la pandemia COVID19 (*ex multis*, Consiglio di Stato, sez. III, 20 ottobre 2021, n. 7045).

18 De Pretis 1995: 11; Fraenkel-Haeberle 2005: 808.

I concetti giuridici indeterminati sono una categoria molto sviluppata nel diritto tedesco (*unbestimmte Rechtsbegriffe*), che in quell'ordinamento consentono una valutazione amministrativa pressoché pienamente sindacabile dal giudice[19]. La categoria nazionale corrispondente, ossia la discrezionalità tecnica, si presenta invece molto più problematica per le note oscillazioni e difficoltà del giudice amministrativo tra sindacato esterno e sindacato interno debole dell'agire amministrativo[20].

Ma anche a livello costituzionale, dove sono posti i primi e fondamentali limiti ai poteri di sicurezza ricorre il riferimento a tali categorie concettuali. La Costituzione, infatti, afferma la possibilità di limitare le libertà da essa espresse solo per preservare "interessi essenziali" al mantenimento di una ordinata convivenza civile[21]. Il limite non è definito precisamente nei suoi termini sostanziali, ma viene costruito con garanzie procedurali e di metodo, quali la riserva di legge, di giurisdizione e l'applicazione dei principi di ragionevolezza e proporzionalità.

3. La poliedricità della sicurezza come concetto olistico e la 'nuova' cybersicurezza

L'inerenza della funzione di sicurezza a tutta l'attività statale e pubblica ne comporta diverse declinazioni e una estrema ampiezza. Accanto alla "sicurezza nazionale", intesa come difesa degli interessi dello Stato come ordinamento di libere istituzioni e comunità (art. 117, II c., lett. d), Cost.), troviamo la sicurezza pubblica in senso materiale e individuale, come ordine pubblico (art. 117, II c., lett. h), Cost.) anche in senso economico[22].

Si tratta di poli diversi della stessa funzione, tra i quali trova spazio la nuova funzione volta a garantire la cybersicurezza, definita nel Cybersecurity Act europeo 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"[23]. La portata di questa definizione non è esigua come a prima vista appare. La rete e i sistemi informativi sono oggi irrinunciabili per il funzionamento dei sistemi statali, intesi in termini istituzionali e delle pubbliche ammi-

19 Fraenkel-Haeberle 2005: 811; Reinhardt 2019: 195.

20 Travi 2001: 9; Villata e Ramajoli 2007: 117.

21 Così Corte cost. sent. 7 aprile 1995, n. 115, in tema di riforma del TUPS; Id. sent. 30 luglio 2020, n. 177, sulla l.r. Puglia n. 14/2019 (Testo unico in materia di legalità, regolarità amministrativa e sicurezza).

22 V. Corte cost., sent. n. 6 luglio 1966, n. 87, punto 4 del *Diritto*. La sentenza, di accoglimento parziale, rigetta la questione costituzionale posta sul divieto penale di propaganda sovversiva ed antinazionale, ritenendo che la disposizione tuteli "l'ordine economico, rispetto al diritto al lavoro, alla organizzazione sindacale, alla iniziativa economica privata, alla proprietà" nonché "il mantenimento dell'ordine pubblico considerato come ordine legale costituito".

23 Art. 2, n. 1), Regolamento (UE) 2019/881 del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("Regolamento sulla cybersicurezza").

nistrazioni[24] ma anche come costruzioni economico-sociali e produttive[25]. Ed è infatti su questi fattori che nell'ultimo decennio si sono trasferite molte delle più incisive minacce alla sicurezza nazionale, delineata come concetto non solo poliedrico ma piuttosto 'olistico', comprensivo cioè di tutti gli aspetti che caratterizzano gli Stati contemporanei e la loro tendenza alla "securitizzazione" della società e dell'ordinamento, nell'ottica di prevenzione della vulnerabilità della società e degli individui per creare resilienza, secondo dinamiche che focalizzano sull'aspetto della protezione anziché su quello della libertà[26].

Così anche il recente regolamento UE sui servizi digitali, che riferisce la sicurezza sia a una dimensione individuale, sia in relazione agli effetti negativi reali o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica in senso materiale[27].

Tale evoluzione rende la cybersicurezza un presupposto di legittimazione di poteri normativi e amministrativi formidabili. Gli strumenti della cybersicurezza sono gli strumenti tradizionali del diritto amministrativo, ma in una declinazione nuova, soprattutto in relazione ai procedimenti e agli organi competenti, come si vedrà nei prossimi paragrafi.

4. Il perimetro di sicurezza nazionale cibernetica: funzione e soggetti inclusi

Il perimetro di sicurezza nazionale cibernetica comprende molti di questi strumenti che si estendono e mescolano con la dimensione economica delle attività private e dello Stato. Esso è stato delineato da un complesso sistema di interventi normativi, europei e nazionali, e provvedimenti d'urgenza nazionali[28].

24 Montessoro 2019: 783; Lauro 2021: 529.

25 Cfr. Angelini e Altri 2021: 7.

26 Buzan e Wæver e De Wilde 1998: 12; Buzzacchi 2015: 104.

27 Regolamento (Ue) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

28 A partire dalle Direttive NIS-1 (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) e NIS-2 (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). Possono essere poi ricordati il richiamato Regolam. UE 2022/2065 sui servizi digitali; il Regolamento (Ue) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione; il d.l. 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica; il dPCM 30 luglio 2020, n. 131 sul Perimetro nazionale di sicurezza cibernetica e il d.l. 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. Più in dettaglio Buoso 2023: 87 ss.; Rossa 2023: 115 ss.

Lo scopo di questo strumento è indicato dall'art. 1 d.l. 105/19. Il perimetro è istituito per

> assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

I richiamati interessi, assolutamente primari, giustificano poteri estremamente ampi ed effetti limitativi dell'iniziativa economica e dell'agire privato, che conseguono all'inserimento di un soggetto e di una attività nel perimetro. Tali limitazioni e conformazioni delle sfere giuridiche dei soggetti individuati, sono accompagnate da alcune peculiarità del procedimento amministrativo che riguarda l'inserimento nel perimetro.

Partendo dall'indicazione dei soggetti sottoposti a questo potere, si tratta di una platea molto ampia, definita secondo un meccanismo articolato in tre presupposti. Il primo è la natura del soggetto, che può essere pubblico (pubbliche amministrazioni e operatori pubblici in senso lato) o privato che abbia una sede nel territorio nazionale; il secondo considera l'attività svolta (tramite reti, sistemi informativi e servizi informatici)[29]. Infine, vengono indicati gli scopi e gli effetti dell'attività da proteggere: da essa, infatti, deve dipendere "una funzione essenziale dello Stato", o "la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato" quando dal loro malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa "derivare un pregiudizio per la sicurezza nazionale".

Qualche specificazione aggiuntiva deriva dal decreto attuativo della norma, ove vengono individuati come soggetti che svolgono "funzioni o servizi essenziali" quelli cui "l'ordinamento attribuisce compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia […] la funzionalità dei sistemi economico e finanziario e dei trasporti"[30]. Quanto ai soggetti che "presta[no] un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato", essi sono inseribili nel perimetro quando pongono in essere attività "strumentali all'esercizio di funzioni essenziali dello Stato; necessarie per

29 Reti e sistemi informativi sono definiti dalle direttive NIS-1 e NIS-2 e del d.lgs. 65/2018, come "qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione".

30 D.P.C.M. n. 131/2020, art. 2 c. 1, lett. a).

l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale"[31].

Le norme distinguono quindi tra "funzioni essenziali dello Stato" – concetto che richiama le "funzioni essenziali dell'ordinamento" individuate dalla giurisprudenza costituzionale come oggetto della funzione di sicurezza[32] – e prestazione di "servizi essenziali" per le attività civili, sociali ed economiche, indicazione che rinvia, anche nell'ordine espositivo, ai diritti garantiti nei primi tre Titoli della parte I della Costituzione.

L'individuazione dei soggetti richiede una operazione ermeneutica quasi heideggeriana, che mette in connessione il destinatario con lo scopo stesso del potere e con una qualificazione dei pericoli e delle minacce da scongiurare.

Guardando alle categorie sviluppate nell'ambito dei principi di precauzione e di prevenzione all'agire anticipatorio della pubblica amministrazione, possiamo chiederci se il presupposto che legittima l'attivazione del potere sia il pericolo (concreto) o il mero rischio (potenziale)[33]. Secondo i criteri di questa dogmatica, a fronte della gravità delle minacce e dell'importanza degli interessi coinvolti, è possibile ritenere sufficiente il mero rischio per attivare il potere amministrativo, con un approccio di estrema prudenza – il medesimo applicato dal legislatore europeo in materia di intelligenza artificiale[34] – decisamente ampliativo del potere. In questo senso depone anche la specificazione normativa, per la quale solo nel caso dei servizi essenziali vengono qualificati gli effetti del malfunzionamento rilevanti per l'inserimento nel perimetro, non invece per le funzioni essenziali.

Le norme italiane non si esprimono in termini di rischio o pericolo, ma il decreto n. 131/2020 sembra richiamare – con confusione di termini – il primo, laddove definisce il pregiudizio per la sicurezza nazionale in termini di

> danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale.

31 Art. 2 c. 1, lett. a), d.P.C.M. n. 131/2020.

32 Ad. es. Corte cost. 25 febbraio 1988, n. 218.

33 Tali categorie sono state sviluppate con ampia elaborazione dottrinale nel sistema tedesco e riconducono rispettivamente al principio di precauzione e a quello di prevenzione: v., per tutti, Breuer 1978: 836; Darnstadt 1983: 6 ss.

34 AI ACT, 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.

Un ulteriore ampliamento dei presupposti di attivazione di questo potere preventivo si ha con l'art. 1 d.l. n. 82/2021, il quale mira a garantire la "resilienza"[35] dei sistemi informativi "anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico". Non risulta peraltro chiaro rispetto a cosa questi elementi si qualifichino come ulteriori; inoltre torna alla luce il tradizionale concetto di interesse nazionale, che la riforma del Titolo V ha estromesso dalla Costituzione[36].

Già questa rapida analisi delle minacce individuate dalle norme come presupposti di esercizio del potere rende evidente come si tratti di rischi che comportano e legittimano una concentrazione di poteri al vertice politico istituzionale dell'esecutivo, perché toccano l'esistenza dello Stato e lo svolgimento delle sue funzioni essenziali. Tale accentramento in capo all'esecutivo e al suo vertice non è privo di risvolti problematici[37] ed è stato temperato rispetto alla versione originaria, che concentrava molte funzioni sul Presidente del Consiglio dei Ministri in coerenza con il suo ruolo di direzione e responsabilità per le politiche di cybersicurezza[38], compartendole con altri organi e con la novella Agenzia nazionale per la cybersicurezza[39] secondo una "geometria variabile" molto articolata[40].

5. Segue: effetti dell'inserimento nel perimetro

L'inclusione di un soggetto nel perimetro nazionale di cybersicurezza comporta obblighi e adempimenti di diversa natura.

Anzitutto scattano obblighi preventivi, che possono essere organizzati in quattro categorie: di comunicazione[41]; di adeguamento delle tecnologie e dei processi interni[42]; di formazione e consapevolezza dei dipendenti[43] e riguardanti gli approvvigionamenti e l'affidamento di forniture di beni, sistemi e servizi di ICT[44].

35 Sul concetto di cyberresilienza, v. Rossa 2023: 72 ss.

36 Barbera 1973: 25 ss.; Tosi 2002: 86.

37 Previti 2022: 65 ss.

38 Sulla strategia nazionale di cybersicurezza, v. Matassa 2022: 625.

39 Cfr. l'art. 1, c. 2 *bis*, d.l. n. 105 del 2019 e i successivi artt. 5 d.P.C.M. n. 131 del 2020 e 7, c. 1, lett. h), d.l. n. 82 del 2021, ai sensi del quale l'ACN assume tutte le funzioni attribuite alla Presidenza del Consiglio dei Ministri di cui al d.l. n. 105 del 2019.

40 Giupponi 2024: 295.

41 Che prevedono la trasmissione all'ACN di un elenco, periodicamente aggiornato, delle reti, dei sistemi informativi e dei servizi informatici: art. 1, comma 2, d.l. n. 10 del 2019. Tale comunicazione consente allo Stato una mappatura totale della struttura dei servizi.

42 Gli adeguamenti devono garantire elevati livelli di sicurezza e relativi diversi tipi di contenuti e attività, secondo uno schema già collaudato con la normativa anticorruzione. Deve inoltre essere creata una struttura organizzativa preposta alla gestione della sicurezza, individuando politiche di gestione del rischio e prevenzione degli incidenti, anche attraverso interventi sugli apparati o sui prodotti che risultino gravemente inadeguati sul piano della sicurezza. Cfr. l'art. 1, c. 3, lett. b), d.l. n. 105 del 2019.

43 Art. 1, comma 3, lett. b), n. 7, d.l. n. 105 del 2019.

44 Art. 1, comma 3, lett. b), n. 8 e c. 6, d.l. n. 105 del 2019. Le disposizioni prevendono

In secondo luogo, sul soggetto all'interno del perimetro pesano obblighi successivi. Al verificarsi di una "compromissione" – definita come perdita di sicurezza o di efficacia dello svolgimento di una funzione essenziale dello Stato o di un servizio essenziale, connessa al malfunzionamento, all'interruzione, anche parziali, ovvero all'utilizzo improprio di reti, sistemi informativi e servizi informatici – o di un "incidente" – ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici-[45] i soggetti del perimetro devono attuare le misure di mitigazione e gestione degli incidenti secondo i protocolli di intervento e notificare l'accaduto al Gruppo di intervento per la sicurezza informatica in caso di incidente istituito presso la ACN[46].

Gli obblighi sono muniti di sanzioni amministrative pecuniarie, da moderate a ingenti[47], lontane dalle soglie massime di altri apparati sanzionatori del diritto amministrativo, probabilmente per evitare che l'eccessiva deterrenza porti a fenomeni di elusione delle comunicazioni, soprattutto in materia di compromissioni e incidenti.

6. Il procedimento di inserimento nel perimetro

Il procedimento – le norme parlano significativamente di procedura[48] quasi a marcare la distanza dal procedimento amministrativo ai sensi della legge generale 7 agosto 1990, n. 241 – di inserimento nel perimetro presenta alcune interessanti peculiarità[49]. Esso si articola in tre passaggi: il primo prevede un sistema di raccolta dei profili da parte dei Ministeri, nei propri settori di attività, come individuati dall'art. 3 d.P.C.M. n. 131/20[50]. Successivamente, l'elenco risultante viene trasmesso al CISR tecnico e sottoposto al CISR "ordinario"[51]. È poi proprio quest'ultimo

sia la definizione di caratteristiche e requisiti di carattere generale, standard e limiti per le acquisizioni, sia l'obbligo di comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN) dell'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici".

45 Per queste definizioni, v. l'art. 1, c. 1, lett. g) e h), d.P.C.M. n. 131 del 2020. L'ACN definisce con propria determinazione la "*tassonomia degli incidenti*" che devono essere oggetto di notifica, come previsto dalla direttiva NIS, e di quelli che possono esserlo, ai fini di "*fornire all'ACN un quadro di valutazione della minaccia più completo*": così la determinazione ACN del 3 gennaio 2023, in G.U. n. 7 del 10 gennaio 2023.

46 Art. 1, comma 3, lett. a), d.l. n. 105 del 2019.

47 Art. 1, comma 9, d.l. n. 105 del 2019

48 Art. 4 d.P.C.M. n. 131/2020.

49 Artt. 1, c. 2, lett. a) d.l. n. 105 del 2019 e 5 d.P.C.M. n. 131/2020.

50 Tali settori sono: a) interno; b) difesa; c) spazio e aerospazio; d) energia; e) telecomunicazioni; f) economia e finanza; g) trasporti; h) servizi digitali; i) tecnologie critiche; l) enti previdenziali/lavoro.

51 Il Comitato interministeriale per la sicurezza della Repubblica è stato istituito ed è disciplinato dall'art. 5 l. 3 agosto 2007, n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto. Il Comitato è coadiuvato da un organismo tecnico

a formulare la proposta di elenco definitivo, che sarà adottato con atto del Presidente del Consiglio dei Ministri[52].

L'individuazione dei soggetti e il loro inserimento nel perimetro si sono così perfezionati, ma ancora nulla è uscito all'esterno né i soggetti inclusi ne hanno contezza. Solo entro 30 giorni dalla conclusione del procedimento il DIS (Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri)[53], comunica – in forma non specificata dalla disposizione – l'avvenuta inclusione al soggetto, indicando la funzione essenziale o il servizio essenziale che giustifica l'inserimento[54].

Evidenti ragioni di sicurezza impediscono la pubblicazione degli atti ma è escluso anche l'accesso, con previsione che limita fortemente le possibilità di opposizione all'inserimento e che va forse differenziata, in via interpretativa, rispetto ai diversi tipi di accesso e ai soggetti richiedenti[55].

Da questo momento devono ritenersi efficaci per i soggetti inclusi nel perimetro gli obblighi sopra ricordati, ma restano poco chiari gli eventuali obblighi di comunicazione ai soggetti connessi (i fornitori etc.) nella rete.

7. I criteri per l'inserimento nel perimetro, la natura del potere e la questione delle garanzie e delle tutele

Sulla base dei presupposti che lo legittimano, degli organi coinvolti nel procedimento e della stessa procedura di compilazione degli elenchi, risulta evidente l'ampiezza delle valutazioni e conseguentemente del potere esercitato, con effetti di vincolo anche molto penetranti sull'attività inclusa nel perimetro.

Le disposizioni specificano un criterio per la formazione dell'elenco e per l'esercizio dei poteri sfavorevoli connessi: la gradualità, in base alla quale si deve tener conto "dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei si-

di supporto, il CISR tecnico (art. 4, c. 5, d.P.C.M. 3 aprile 2020, n. 2), istituito presso il DIS, presieduto dal Direttore Generale e composto dai direttori delle Agenzie e da Dirigenti apicali designati dai Ministri membri del CISR. In proposito Vigna 2007: 693; Bellandi 2013: 1.

52 Artt. 1, c. 2-bis, d.l. 105/2019. Il d.l. n. 82/2021 parrebbe però aver trasmesso anche questa competenza all'ACN.

53 Art. 4 l. 3 agosto 2007, n. 124.

54 Artt. 1, c. 2-bis d.l. 105/2019 e 5, c. 3, d.P.C.M. n. 131/2020. La disposizione regolamentare specifica una serie di ulteriori informative: l'avvenuta iscrizione è comunicata anche alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, per i soggetti pubblici e per quelli di cui all'articolo 29 del codice dell'amministrazione digitale, e al Ministero dello sviluppo economico, per quelli privati. Inoltre, l'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica è trasmesso all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (previsto dall'art. 7-bis d.l. 27 luglio 2005, n. 144, conv. con modif. in l. 31 luglio 2005, n. 155).

55 Art. 1, c. 2-bis, d.l. n. 105/2019.

stemi informativi e dei servizi informatici predetti"[56]. Nonostante il termine non compaia, si tratta di una descrizione del concetto di proporzionalità, inteso non come principio ma come canone di decisione amministrativa[57], declinato alla luce delle valutazioni di costi-benefici e delle regole di *risk assesment*[58].

Ci si può chiedere, pertanto, se l'applicazione del criterio di gradualità non sia già necessitata per il nostro diritto amministrativo e la sua formulazione non risulti troppo generale per costituire una linea guida ulteriore. A questo proposito sarebbe opportuna una maggiore specificazione delle categorie di attività, seguendo l'approccio *risk oriented* del Regolamento UE dei servizi digitali e del Regolamento AI, che elencano diverse categorie di rischio sistemico, mappate e valutate dai gestori, sulle quali si graduano gli obblighi.

L'atto di inserimento nel perimetro, tramite la predisposizione degli elenchi, è esercizio di un potere di prevenzione che si situa ad un crocevia tra atto di indirizzo, valutazione tecnica e scelta discrezionale, che – negli effetti – sembra avvicinabile all'imposizione di un vincolo, costitutivo, conformativo e compressivo della situazione giuridica soggettiva del soggetto inserito. La coesistenza di valutazione tecnica – espressa dal contributo alla compilazione degli elenchi fornito dai Ministeri e dal CISR tecnico – assieme a una componente di discrezionalità amministrativa pura rende necessario ma anche possibile un bilanciamento tra la tutela di interessi pubblici essenziali in gioco con quelli privati o pubblici contrastanti.

Le usuali garanzie per un corretto bilanciamento, anche in vista della tutela giurisdizionale successiva, tradizionalmente offerte nel nostro ordinamento dal procedimento, sono molto poche. Prevale, infatti, l'esigenza di sicurezza, sacrificando quelle di trasparenza e partecipazione.

La formulazione normativa consente di ipotizzare un atto di inserimento la cui motivazione si sostanzia nell'indicazione della funzione e del servizio essenziale offerto dall'operatore, quindi pressoché non sindacabile, salvo macroscopici travisamenti.

Un limite può essere offerto dai criteri sostanziali che sono alla base delle valutazioni di tipo tecnico per la formazione degli elenchi, anche in ambiti ad alta sensibilità politico-economica. Ma le formulazioni generali e la mancata applicazione del diritto di accesso, se applicata in riferimento a tutte le sue forme, compreso l'accesso documentale del soggetto incluso, può rendere molto difficile l'individuazione di queste valutazioni e la loro giustiziabilità.

La garanzia più efficace, ad oggi, sembra risiedere nell'aspetto organizzativo della architettura della cybersicurezza in Italia. Rispetto alla disciplina originaria è stato introdotto un sistema di condivisione e di gestione del potere attraverso strutture organizzative complesse e coordinate dei vari Ministeri e di altri organi, nonché dal ruolo – non ancora del tutto definito – della Agenzia nazionale.

56 Art. 1, c. 2, d.l. 105/19 e art. 3 d.P.C.M. n. 131/2020.

57 Buoso 2012: 255.

58 Su questi aspetti della proporzionalità per una obiettiva valutazione del rischio, v. Schrader-Frechette 1993: 91 ss.

Se queste garanzie siano sufficienti per bilanciare un potere non nuovo nella sua natura ma inedito nelle modalità di esercizio[59], è ancora presto per dirlo. La cifra e la gravità delle minacce giustificano le nuove forme di potere preventivo, ma è necessario vigilare perché non divengano occasione per un ritorno al passato, ai poteri di una amministrazione quasi ottocentesca con i potenziati sistemi di controllo che la tecnologia consente[60]. Il viaggio dell'ordinamento, con il bagaglio delle categorie tradizionali della sicurezza, deve invece puntare al futuro.

Bibliografia

Angelini M. e Altri 2021, *Metodologia per il cybersecurity assesment con il Framework Nazionale per la Cybersecurity e la Data Protection*, disponibile al sito *http://www.cybersecurityfracamework.it* (consultato il 18 luglio 2024).

Barbera A. 1973, *Regioni e interesse nazionale*, Milano: Giuffrè.

Barile P. 1967, "La pubblica sicurezza", in Id. (a cura di) 1967, *La pubblica sicurezza*, Vicenza: Neri Pozza.

Barone A. 2006, *Il diritto del rischio*, Milano: Giuffrè.

Bauman Z. 2006, *Liquid Fear*, Hoboken: Wiley.

Beck U. 1986, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt am Main: Suhrkamp.

Bellandi R. 2013, "L'affermazione del Comitato interministeriale per la Sicurezza della Repubblica (CISR) quale nuovo protagonista della politica di sicurezza nazionale", in *federalismi.it*, 24: 1-15.

Bifulco L. 2018, "La sicurezza negli stadi in Italia. Tifo, violenza, diritto e misure di contrasto", in *Sociologia del diritto*, 3: 159-185.

Braml J. 2021, "Anti-terrorism laws and powers. An inventory of the G20 States 20 years after 9/11", in *Friedrich Ebert Stiftung*. Disponibile al link https://ny.fes.de/article/anti-terrorism-laws-20-years-after-9-11.html (ult. accesso: June 30, 2024).

Breuer R. 1978, "Gefahrenabwehr und Risikovorsorge im Atomrecht", in *Deutsches Verwaltungsblatt.*, 836-852.

Buoso E. 2012, *Proporzionalità, efficienza e accordi nell'attività amministrativa*, Padova: CEDAM.

Buoso E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli.

Buzan B., Wæver O., De Wilde J. 1998, *Security: A New Framework for Analysis*, Boulder-London: Lynne Rienner.

Buzzacchi C. 2015, "Sicurezza e securitization tra Stato, Unione europea e mercato", in Pizzolato F. e Costa P. (a cura di) 2015, *Sicurezza, Stato e mercato*, Milano: Giuffrè, 98-131.

Caia G. 2000, "L'ordine e la sicurezza pubblica", in Cassese S. (a cura di) 2000, *Trattato di diritto amministrativo*, Milano: Giuffrè.

Carotti B. 2020, "Sicurezza cibernetica e Stato-nazione", in *Giornale di Diritto Amministrativo*, 5: 629-641.

Cassese S. 2000, *Le basi del diritto amministrativo*, VI ed., Milano: Giuffrè.

Cassese S. 2010, *Lo Stato fascista*, Bologna: Il Mulino.

59 Ursi 2023: 7 ss.

60 Su questi aspetti, v. Carotti 2020: 639.

Cerrina Feroni G. e Morbidelli G. 2008, "La sicurezza: un valore superprimario", in *Percorsi costituzionali*, 1: 31-44.
Chiti E. 2016, "Le sfide alla sicurezza e gli assetti nazionali ed europei delle forze di sicurezza e di difesa", in *Diritto amministrativo*, 4: 511-547.
Corso G. 1979, Corso G., *L'ordine pubblico*, Bologna: Il Mulino.
D. de Pretis 1995, *Valutazione amministrativa e discrezionalità tecnica*, Padova: CEDAM.
D'Arienzo M. 2012, "Divieto di accesso alle manifestazioni sportive (daspo): natura, funzione e problematiche connesse alla sua applicazione", in *Diritto e processo amministrativo*, 4: 1311-1329.
D'Atena A. 2018, "Costituzionalismo e tutela dei diritti fondamentali", in Id. 2018 [2001], *Lezioni di diritto costituzionale*, Torino: Giappichelli.
Darnstadt T. 1983, *Gefahrenabwehr und Gefahrenvorsorge: eine Untersuchung über Struktur und Bedeutung der Prognose-Tatbestände im Recht der öffentlichen Sicherheit und Ordnung*, Frankfurt a. M.: Metzner.
de Leonardis F. 2005, *Il principio di precauzione nell'amministrazione di rischio*, Giuffrè: Milano.
Di Nella L. 2018, "La violenza negli stadi. L'esperienza tedesca", in *Rassegna di diritto ed economia dello sport*, 1: 77-93.
Fisichella D. 2008, *Alla ricerca della sovranità. Sicurezza e libertà in Thomas Hobbes*, Roma: Carocci.
Follieri E. 2017, "Il daspo urbano (artt. 9, 10 e 13 del D.L. 20.2.2017 n. 14)", in *GiustAmm. it*, 3: 23-49.
Fraenkel-Haeberle C. 2005, „Unbestimmte Rechtsbegriffe, technisches Ermessen und gerichtliche Nachprüfbarkeit – Eine rechtsvergleichende Analyse", in *Die Öffentliche Verwaltung*, 808-815.
Garaffa P. 2018, "Misure antiviolenza negli stadi: vecchi e nuovi contrasti, vecchie e nuove questioni, vecchi e nuovi chiarimenti", in *La Giustizia Penale*, 7: 399-448.
Giupponi T. 2024, "Il governo nazionale della cybersicurezza", in *Quaderni costituzionali*, 2: 277-303.
Groppali A. 1940, "Sul concetto di ordine pubblico", in AA.VV. 1940, *Scritti giuridici in onore di Santi Romano*, vol. II, Padova: CEDAM.
Haubrich D. 2003, "September 11, Anti-Terror Laws and Civil Liberties: Britain, France and Germany Compared", in *Government and Opposition*, 38(1): 3-28.
Kipker D-K. and Pagel P. 2020, "Editorial", in *International Cybersecurity Law Review – Zeitschrift für Cybersicherheit und Recht*, 1: 1-5.
Lauro A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *Quaderni del Gruppo di Pisa*, 3: 529-545.
Luhmann N. 1991, *Soziologie des Risikos*, Berlin-New York: Walter de Gruyter.
Maggio P. 2013, "La lotta alla criminalità organizzata in Europa fra strategie di contrasto e rispetto dei diritti umani", in *Cassazione penale*, 2: 808-821.
Manfredi G. 2011, "Cambiamenti climatici e principio di precauzione", in *Rivista quadrimestrale di diritto dell'ambiente*, 27-39.
Matassa M. 2022, "Una strategia nazionale a difesa del cyberspazio", in *Persona e amministrazione*, 2: 625-653.
Matteucci N. 2016, *Organizzazione del potere e libertà. Storia del costituzionalismo moderno*, Bologna: Il Mulino.
Mazzamuto M. 2018, "Le interdittive prefettizie tra prevenzione antimafia e salvataggio delle imprese", in *Giurisprudenza italiana*, 10: 2222-2230.
Montessoro P.L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti dell'amministrazione digitale", in *Istituzioni del federalismo*, 3: 783-800.

Mortati C. 1975, *Istituzioni di diritto pubblico*, vol. I, Padova: CEDAM.
Napolitano G. 2014, "Diritto amministrativo e processo economico", in *Diritto amministrativo*, 4: 695-724.
Orlando V.E. 1904, "Introduzione al Diritto amministrativo", in Id., (a cura di) 1904, *Primo trattato completo di diritto amministrativo italiano*, vol. I, Milano: Società editrice libraria.
Panza G. 1990, "Ordine pubblico, I) Teoria generale", in *Enc. giur*., XXII, Roma: Treccani.
Passarelli t. 2024, "Interdittive antimafia e prevenzione collaborativa: azioni di contrasto al crimine organizzato tra incertezze legislative e discrezionalità applicativa", in *federalismi.it*, 10: 150-173.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informativo", in *federalismi.it*, 25: 65-93.
Prosperi A. 2016, "L'esperienza della storia italiana, antica e recente", in *Terrorismo internazionale. Politiche della sicurezza. Diritti fondamentali – Speciale di Questione Giustizia*, 16-25. Disponibile al link https://www.questionegiustizia.it/speciale/2016-1 (consultato il 5 luglio 2024).
Raimondi S. 2023, *La sicurezza pubblica*, Torino: Giappichelli.
Ranelletti O. 1904, "La polizia di sicurezza", in Orlando V.E. (a cura di) 1904, *Primo trattato completo di diritto amministrativo italiano*, vol. IV, Milano: Società editrice libraria.
Reinhardt M. 2019, „Umweltschutz ist wesentlich. Verfassungsrechtliche Anforderungen an die Standardsetzung mit unbestimmten und unbestimmbaren Rechtsbegriffen", in *Neue Zeitschrift für Verwaltungsrecht*, 195-211.
Romano S. 1912 [1901], *Principii di diritto amministrativo italiano*, Milano: Società editrice libraria.
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica.
Schrader-Frechette K.S. 1993, *Valutare il rischio*, trad. it., Milano: Giuffrè.
Schwegel A. 2005, *Der Polizeibegriff im NS-Staat*, Tübingen: Mohr Siebeck.
Sciullo G. 2016, "'Interessi differenziati' e procedimento amministrativo", in *Rivista giuridica di urbanistica*,1: 58-98.
Spataro A. 2023, "Il contrasto al terrorismo", in *Sistema penale*, 1-26.
Sticchi Damiani S. e Amarelli G 2016, *Le interdittive antimafia e le altre misure di contrasto all'infiltrazione mafiosa negli appalti pubblici*, Torino; Giappichelli.
Tonoletti B. 2022, "Ordine e sicurezza pubblica", in Mattarella B.G. e Ramajoli M. (a cura di) 2022, *Funzioni amministrative – Enciclopedia del diritto. I Tematici*, III, Milano: Giuffrè, 791-816.
Tosi R. 2002, "A proposito dell'interesse nazionale", in *Quaderni costituzionali*, 86-88.
Travi A. 2001, "Circa il sindacato del giudice amministrativo sulla discrezionalità tecnica della pubblica amministrazione", in *Foro it.*, III, 9-15.
Trimarchi F. 2005, "Principio di precauzione e «qualità» dell'azione amministrativa", in *Rivista trimestrale di diritto pubblico e comunitario*, 1673-1707.
Tropea G. 2010, *Sicurezza e sussidiarietà. Premesse per uno studio sui rapporti tra sicurezza pubblica e democrazia amministrativa*, Edizioni Scientifiche Italiane: Napoli.
Ursi R. 2022, *La sicurezza pubblica,* Bologna: Il Mulino.
Ursi R. 2023, "La sicurezza cibernetica come funzione pubblica", in Id. (a cura di) 2023, *La Sicurezza nel Cyberspazio*, Milano: Franco Angeli, 7-20.
Vigna P.L. 2007, "La nuova disciplina dei servizi di sicurezza", in *La Legislazione penale*, 4(2): 693-702.
Villata R. e Ramajoli M. 2007, *Il provvedimento amministrativo*, Torino; Giappichelli.

Giovanna Dondossola

Impatto della Legislazione di Cybersecurity sulla Normativa per il controllo di risorse energetiche[*]

Abstract: L'utilizzo diversificato di energia rinnovabile e l'elettrificazione dei trasporti e del riscaldamento introducono una trasformazione digitale delle infrastrutture energetiche che richiede una gestione dei rischi derivanti dalle minacce alla cybersecurity. Lo sviluppo e l'adozione di misure di cybersecurity adeguate al livello di rischio dell'infrastruttura energetica cyber-fisica è una priorità riconosciuta dalle strategie di sviluppo e innovazione del sistema paese, finalizzate a garantire un livello di maturità tecnologica allineato ai target di cybersecurity europei e nazionali. Con l'obiettivo di esemplificare il percorso regolatorio che stabilisce misure di cybersecurity per infrastrutture energetiche, questo articolo illustra le caratteristiche principali del processo regolatorio per la cybersecurity degli impianti di generazione connessi alle reti elettriche, il quale prende avvio nel 2017 dalla regolazione elettrica a livello europeo, interseca la legislazione di cybersecurity e si concretizza con l'adozione nel 2023 di standard di cybersecurity internazionali da parte dei suddetti impianti.

Keywords: Cybersecurity; Direttiva NIS2; Perimetro nazionale di sicurezza Cibernetica; Electricity Regulation; Standard internazionali.

1. Processo regolatorio di settore elettrico

Il processo regolatorio del settore elettrico è tipicamente avviato da atti legislativi, denominati Codici di Rete, emanati dalla Unione Europea e successivamente recepiti dagli stati membri.

Il processo regolatorio illustrato in questo articolo, avviato nel 2017 e terminato nel 2023, fa riferimento al Codice di Rete Europeo 2017/1485 *System Operation Guideline* (SOGL)[1] il quale, ai fini della pianificazione e gestione operativa del

* Questo scritto è stato finanziato dal Fondo di Ricerca per il Sistema Elettrico nell'ambito del Piano Triennale 2022-2024 (DM MITE n. 337, 15.09.2022), in ottemperanza al DM 16 aprile 2018.

1 Regolamento EU 2017/1485, stabilisce orientamenti in materia di gestione del sistema di trasmissione dell'energia elettrica, 2017. Disponibile online: REGOLAMENTO (UE) 2017/

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760159

sistema elettrico in tempo reale, stabilisce la necessità di scambio dati tra operatori delle reti di trasmissione e distribuzione dell'energia elettrica e utenti di rete significativi. Il regolamento SOGL è stato recepito dall'Operatore italiano della rete elettrica di trasmissione, Terna, all'interno del Codice di Rete Nazionale, il cui Allegato 6[2] specifica le modalità, i contenuti e i requisiti dello scambio dati relativo ad impianti di generazione connessi alle reti in media tensione, di capacità uguale o superiore ad un megawatt. Il perimetro di applicazione del Codice di Rete contribuisce al raggiungimento degli obiettivi della transizione energetica del Paese stabiliti dal Piano Nazionale Integrato per l'Energia e il Clima (PNIEC), pubblicato nel 2019 e successivamente aggiornato (a giugno 2023) dal Ministero dell'Ambiente e della Sicurezza Energetica[3]. Secondo il PNIEC, nel 2030 l'Italia intende perseguire un obiettivo di copertura del 40,5% del consumo finale lordo di energia da fonti rinnovabili, delineando un percorso di crescita ambizioso di queste fonti con una piena integrazione nel sistema energetico nazionale.

Nel febbraio 2020 l'Autorità italiana per la Regolazione dell'Energia (ARERA) ha approvato le proposte di modifica del Codice di Rete di Terna ed incaricato contestualmente il Comitato Elettrotecnico Italiano (CEI) degli sviluppi normativi per la specifica delle regole di connessione alle reti e delle tecnologie digitali da utilizzare per l'implementazione dello scambio dati tra gli impianti di generazione nel perimetro di applicazione e gli Operatori delle reti di distribuzione (DSO) di competenza.

Prende quindi avvio a cura dei Comitati Tecnici CT 316 "Connessione alle reti elettriche di distribuzione Alta, Media e Bassa Tensione" e CT 57 "Scambio informativo associato alla gestione dei sistemi elettrici di potenza" del CEI il progetto normativo Controllore Centrale di Impianto (CCI), un insieme di funzioni di monitoraggio e controllo degli impianti energetici distribuiti (DER) la cui specifica funzionale e tecnologica è contenuta, rispettivamente negli Allegati O[4] e T[5] della Norma CEI 0-16.

Tenuto conto del quadro legislativo di riferimento per la cybersecurity delle reti informatiche degli operatori energetici illustrato in seguito, la specifica del CCI

1485 DELLA COMMISSIONE – del 2 agosto 2017 – che stabilisce orientamenti in materia di gestione del sistema di trasmissione dell'energia elettrica (europa.eu) (accesso 14 Agosto 2024).

2 Terna, Allegato A.6 del codice di rete Rev. 04, Criteri di acquisizione dati per il telecontrollo, luglio 2022. Disponibile online: https://download.terna.it/terna/20220701_Allegato_A.6_8da5b792cadec35.pdf (accesso 14 Agosto 2024).

3 Piano Nazionale Integrato per l'Energia e il Clima, Ministero dell'Ambiente e della Sicurezza Energetica, Giugno 2023. Disponibile online: https://www.mase.gov.it/sites/default/files/PNIEC_2023.pdf (accesso 14 Agosto 2022).

4 CEI 0-16:2022-03, Regola Tecnica di Riferimento per la Connessione di Utenti Attivi e Passivi alle reti AT e MT delle Imprese Distributrici di Energia Elettrica. CEI, Milano, Italy. 2022. Disponibile online: https://static.ceinorme.it/strumentionline/doc/18308.pdf (accesso 14 Agosto 2024).

5 Variante V2 della Norma CEI 0-16:2022-03, Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT e MT delle imprese distributrici di energia elettrica, 2023. Disponibile online: https://static.ceinorme.it/strumenti-online/doc/20402.pdf (accesso 14 Agosto 2024).

ha indirizzato i requisiti di cybersecurity attraverso l'applicazione degli standard internazionali ISA/IEC 62443[6,7] e IEC 62351[8].

Nel 2021 ARERA emette la Delibera 540/2021/R/EEL[9] la quale impone l'obbligatorietà delle funzioni di osservabilità del CCI conformi alla Norma CEI 0-16 per gli impianti di produzione connessi alle reti di media tensione con potenza pari o superiore a un megawatt.

Lo schema complessivo del processo regolatorio appena descritto (dal Codice di Rete SOGL all'implementazione obbligatoria degli standard di comunicazione e sicurezza informatica per le comunicazioni DSO-DER a livello nazionale) è schematizzato in Figura 1, insieme agli attori, agli atti legislativi, agli standard internazionali e alle norme nazionali che sono intervenuti nelle diverse fasi del processo.

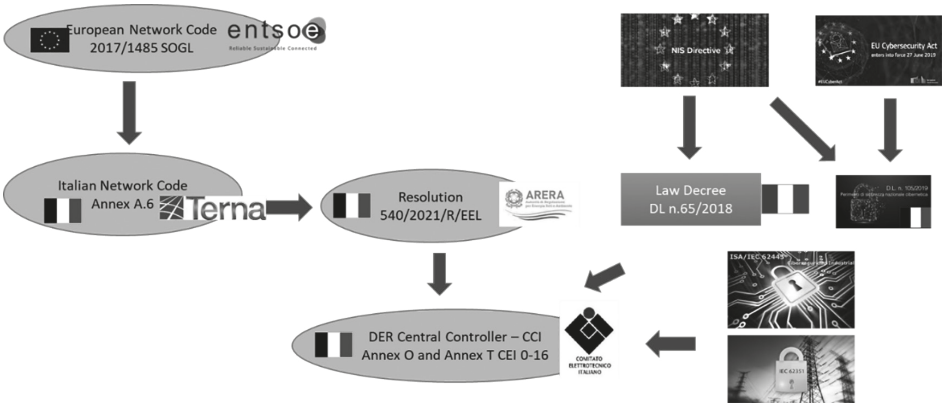


Figura 1 – Schema e attori del processo regolatorio

Nelle sezioni che seguono vengono illustrati gli aspetti salienti della legislazione sulla cybersecurity, a livello Europeo e Nazionale, e il loro recepimento nei requisiti e nelle tecnologie del Controllore Centrale di Impianto.

6 ISA/IEC 62443-4-1, Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. Available online: https://webstore.iec.ch/en/publication/33615 (access on 14 August 2024).

7 IEC 62443-4-2:2019, Security for Industrial Automation and Control Systems-Part 4-2: Technical Security Requirements for IACS Components IEC, Geneva, Switzerland, 2019. Available online: https://webstore.iec.ch/en/publication/34421 (access on 14 August 2024).

8 IEC 62351:2024, Power systems management and associated information exchange – Data and communications security – ALL PARTS", 2024. Available online: https://webstore.iec.ch/en/publication/6912 (access on 14 August 2024).

9 ARERA, Regolazione dello scambio dati tra TERNA S.P.A., Imprese Distributrici e Significant Grid Users ai fini dell'esercizio in sicurezza del sistema elettrico nazionale, Deliberazione 540/2021/R/EEL, 30 Novembre 2021. Disponibile online: https://www.arera.it/fileadmin/allegati/docs/21/540-21.pdf (accesso 14 Agosto 2022).

2. La Direttiva europea NIS2 2022/2555

I settori dell'energia rientrano nel perimetro di applicazione della Direttiva Europea NIS2 2022/2555[10] relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, entrata in vigore il 16 gennaio 2023 in sostituzione della precedente Direttiva NIS 2016/1148[11] sulla sicurezza delle reti e dei sistemi informativi.

La NIS2 rinforza lo stato di sicurezza informatica richiesto a tutta l'Europa coprendo una quota più ampia dell'economia e della società. Il campo di applicazione del settore Energia, considerato ad alta criticità, include i sottosettori energia elettrica, teleriscaldamento e teleraffrescamento, petrolio, gas e idrogeno. Per il sottosettore energia elettrica, la direttiva esplicita i seguenti tipi di soggetti interessati (Allegato I):

- le imprese elettriche;
- i gestori dei sistemi di distribuzione e di trasmissione;
- i produttori, quali sono i proprietari degli impianti di generazione interessati dal processo regolatorio descritto in questo articolo;
- i gestori del mercato elettrico;
- i partecipanti al mercato dell'energia elettrica che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia;
- i gestori di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità.

I soggetti, che rientrano nell'ambito di applicazione della NIS2, ai fini del rispetto delle misure di gestione dei rischi di cybersecurity e degli obblighi di segnalazione, vengono classificati in soggetti essenziali e soggetti importanti (Articolo 3) in funzione della loro rilevanza per il settore o il tipo di servizi che forniscono, nonché delle loro dimensioni.

In tema di misure di gestione dei rischi di cibersicurezza, il paragrafo 1 dell'Articolo 21 stabilisce che "Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi".

Le misure di sicurezza tengono conto delle soluzioni più aggiornate e mature e degli standard europei ed internazionali pertinenti per il settore al fine di assicurare un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. La proporzionalità delle misure dipende dal grado di esposizione del soggetto a

10 Direttiva EU 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, 2022. Disponibile online: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555 (accesso 14 Agosto 2024).

11 Direttiva EU 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione 2016. Disponibile online: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148 (accesso 14 Agosto 2024).

rischi, dalle dimensioni del soggetto, dalla probabilità che si verifichino incidenti, dalla loro gravità e dal loro impatto sociale ed economico.

Tra gli aspetti delle misure di sicurezza elencati nel paragrafo 2 dell'Articolo 21, le misure indirizzate dalla Norma CEI 0-16 riguardano:

- sicurezza dell'approvvigionamento dei dispositivi CCI e dei servizi di gestione dei certificati elettronici;
- la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei dispositivi CCI;
- le politiche, le procedure e gli algoritmi di crittografia e di cifratura;
- le soluzioni di controllo degli accessi, delle autorizzazioni e di autenticazione.
- In allineamento con il Regolamento Europeo *Cyber Security Act*[12] e con la proposta di Regolamento Europeo *Cyber Resilience Act* (CRA)[13], la NIS2 fa esplicito riferimento alla conformità a schemi Europei di certificazione della cybersecurity (Articolo 24). Il CRA si applica ai prodotti con elementi digitali il cui uso prevede una connessione dati, diretta o indiretta, logica o fisica, a un dispositivo o a una rete, stabilendo obblighi per i costruttori, i distributori e gli operatori dei prodotti per garantire:
- miglioramenti nella sicurezza di prodotti con elementi digitali durante l'intero ciclo di vita;
- un framework di sicurezza informatica, che facilita la conformità per produttori di hardware e software, favorendone la valutazione della conformità;
- trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali, consentendo alle aziende e ai consumatori di utilizzare prodotti con elementi digitali in modo sicuro.

Il sistema sanzionatorio introdotto dalla NIS2, la cui responsabilità ricade sugli Stati membri, dovrà essere adottato in funzione della tipologia di soggetti (Articolo 34).

3. La legge italiana 2019/105

Il Decreto-Legge 2018/65[14], entrato in vigore il 24 Giugno 2018, costituisce l'attuazione italiana della Direttiva europea NIS[15]. Un primo fondamentale provvedi-

12 Regolamento EU 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, 2019. Disponibile online: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881 (accesso 14 Agosto 2024).

13 Proposta di Regolamento EU relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, 2022. Disponibile online: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0010.02/DOC_1&format=PDF (accesso 14 Agosto 2024).

14 Decreto-Legge 2018/65, attuazione della 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, Gazzetta Ufficiale n.132 del 9-6-2018, 2018. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg (accesso 14 Agosto 2024).

15 Cfr. nota 11.

mento stabilito dal Decreto 2018/65 è relativo all'identificazione degli operatori classificati come fornitori di servizi essenziali, quali quelli energetici, soggetti agli obblighi in materia di sicurezza e notifica degli incidenti indicati dall'Articolo 14, e alle relative sanzioni amministrative in caso di inadempienza di cui all'Articolo 21.

Il successivo Decreto-Legge 2019/105[16] introduce disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

Il perimetro di sicurezza cibernetica riguarda tutte le infrastrutture critiche private e pubbliche, aventi una sede nel territorio nazionale, che assicurano un servizio essenziale per le attività civili, sociali o economiche fondamentali per la nazione, e che per la fornitura di tale servizio si avvalgono di reti, sistemi informativi e servizi informatici dal cui malfunzionamento o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale. Nella legge Perimetro vengono stabilite le misure (legali, organizzative e tecnologiche) di gestione del rischio e di mitigazione e gestione degli incidenti che garantiscono elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici tenendo conto degli standard definiti a livello internazionale ed europeo.

L'attuazione della Legge Perimetro è a carico dell'Agenzia per la Cybersicurezza Nazionale (ACN) istituita dal Decreto-Legge 2021/82[17] del 14/06/2021. ACN è l'Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. L'ACN predispone la strategia nazionale di cybersicurezza ed è Autorità nazionale di certificazione della cybersicurezza**,** secondo quanto specificato dal Parlamento europeo e del Consiglio, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni.

Il Decreto del Presidente della Repubblica (DPR) 2021/54[18] del 5/02/2021, include:

16 Decreto-Legge 2019/105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (e di disciplina dei poteri speciali nei settori di rilevanza strategica), Gazzetta Ufficiale Serie Generale n.222 del 21-09-2019, 2019. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg (accesso 14 Agosto 2024).

17 Decreto-Legge 2021/82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, Gazzetta Ufficiale Serie Generale n.140 del 14-06-2021, 2021. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg (accesso 14 Agosto 2024).

18 Decreto del Presidente della Repubblica 2021/54, Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, Gazzetta Ufficiale Serie Generale n.97 del 23-04-2021, 2021. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/SG (accesso 14 Agosto 2024).

- procedure, modalità e termini di funzionamento del Centro di Valutazione e Certificazione Nazionale (CVCN) trasferito presso ACN;
- criteri tecnici per l'individuazione delle categorie e dell'elenco dei beni, dei sistemi e dei servizi a cui si applica la procedura di valutazione;
- procedure, modalità e termini con cui le autorità competenti effettuano le verifiche.

Il Procedimento di verifica e valutazione dettagliato nell'Articolo 4 del DPR si articola in verifiche preliminari (Articolo 5), fase di preparazione all'esecuzione dei test (Articolo 6); esecuzione dei test di hardware e software (Articolo 7).

All'esito delle verifiche e dei test, il CVCN o i Centri di Valutazione accreditati definiscono eventuali condizioni e test di hardware e di software da inserire nelle clausole del bando di gara o del contratto, nonché eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro.

Il Decreto del Presidente del Consiglio dei Ministri (DPCM) 2021/81[19] del 14/04/2021 introduce il regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici. Il DPCM riporta tre allegati:

1. nell'allegato A sono presenti tabelle che rappresentano, divisi per categoria, gli incidenti aventi impatto sui beni ICT;
2. nell'allegato B sono presenti le misure di sicurezza, articolate in funzioni, categorie, sottocategorie, punti e lettere;
3. nell'allegato C sono presenti le misure minime di sicurezza per la tutela delle informazioni.

Dal 1° gennaio 2022, i soggetti inclusi nel perimetro, al verificarsi di uno degli incidenti avente impatto su un bene ICT di rispettiva pertinenza individuati nelle tabelle di cui all'allegato A, procedono alla notifica al CSIRT italiano secondo le modalità descritte nel decreto.

I soggetti inclusi nel perimetro procedono alla notifica anche nei casi in cui uno degli incidenti individuati nelle tabelle dell'allegato A si verifichi a carico di un sistema informativo o un servizio informatico, o parti di essi, che condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione.

Nella prossima sezione vengono sommariamente descritte le misure di sicurezza dei controllori di impianti di generazione specificate dalla Norma CEI 0-16[20], che ricadono nelle funzioni di sicurezza Protezione (PR) e Rilevamento (DE) indicate nell'Allegato B. In ottemperanza ai requisiti della Legge Perimetro, la Norma prevede il rilascio, da parte di enti di certificazione, di attestati di conformità allo standard dei profili di cybersecurity e di certificazioni di cybersecurity del prodotto CCI.

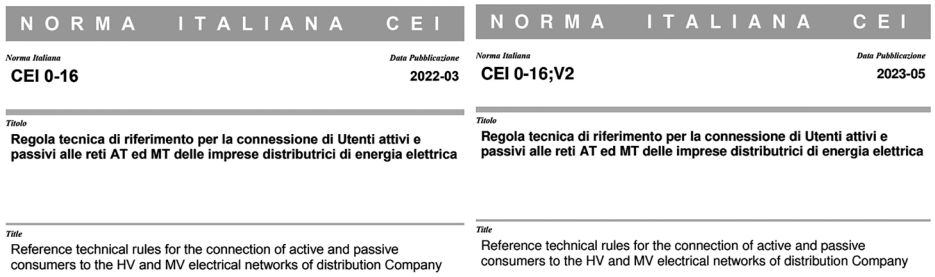
19 Decreto del Presidente del Consiglio dei Ministri 2021/81, Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, Gazzetta Ufficiale Serie Generale n.138 del 11-06-2021, 2021. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/SG (accesso 14 Agosto 2024).

20 Cfr. nota 5.

4. La norma CEI 0-16 e la sicurezza delle comunicazioni dei controllori di impianti di generazione connessi alle reti in media tensione

Per il funzionamento in sicurezza del sistema elettrico, il CCI deve mettere a disposizione una serie di misure e stati di impianto assicurando il dettaglio, la precisione e la periodicità di aggiornamento prescritti dall'Allegato 6 del Codice di Rete Nazionale[21].

Come evidenziato in Figura 1, la specifica del dispositivo CCI e delle sue interfacce di comunicazione è contenuta negli Allegati O[22] e T[23]della Norma CEI 0-16 redatta a cura di esperti dei Comitati Tecnici 316 e 57 del CEI (Figura 2).


NORMA ITALIANA CEI

Norma Italiana **CEI 0-16** *Data Pubblicazione* **2022-03**

Titolo
Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT ed MT delle imprese distributrici di energia elettrica

Title
Reference technical rules for the connection of active and passive consumers to the HV and MV electrical networks of distribution Company

NORMA ITALIANA CEI

Norma Italiana **CEI 0-16;V2** *Data Pubblicazione* **2023-05**

Titolo
Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT ed MT delle imprese distributrici di energia elettrica

Title
Reference technical rules for the connection of active and passive consumers to the HV and MV electrical networks of distribution Company

Figura 2 – Norma CEI 0-16:2022-03 e variante CEI 0-16;V2:2023-05

L'interfaccia di comunicazione DER-DSO definisce un modello dati e protocolli di comunicazione e di cybersecurity conformi agli standard internazionali IEC 61850[24] e IEC 62351[25].

Le funzioni di sicurezza dell'interfaccia DER-DSO, raggruppate secondo la classificazione della Legge Perimetro, sono elencate nel seguito:

- Gestione delle identità, autenticazione e controllo degli accessi (PR.AC): identificazione e autorizzazione delle entità remote basate sulla verifica del certificato elettronico della Autorità di Certificazione, preconfigurato nel CCI, e sul controllo delle autorizzazioni di accesso basato sui ruoli (Figura 3) in conformità allo standard IEC 62351-8[26];

21 Cfr. nota 2.
22 Cfr. nota 4.
23 Cfr. nota 5.
24 IEC 61850:2024, Communication networks and systems for power utility automation – ALL PARTS, 2024. Available online: https://webstore.iec.ch/en/publication/6028 (access on 14 August 2024).
25 Cfr. nota 8.
26 IEC 62351-8, Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management. Available online: https://webstore.iec.ch/en/publication/61822 (access on 14 August 2024).

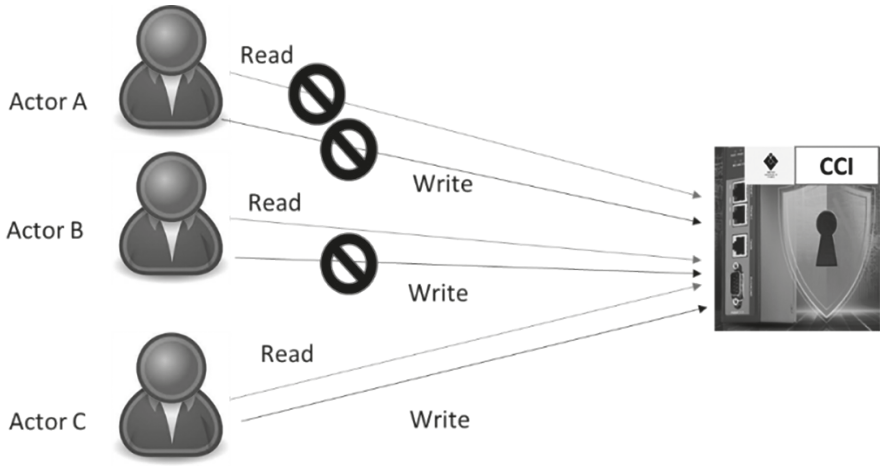


Figura 3 – Controllo delle autorizzazioni di accesso basato sui ruoli

- Sicurezza dei dati (PR.DS): sicurezza delle comunicazioni IEC 61850[27], in conformità agli standard IEC 62351-3[28] e IEC 62351-4[29]. In particolare:
  - mutua autenticazione dei nodi comunicanti mediante certificati elettronici firmati da autorità riconosciute;
  - integrità e confidenzialità dei dati scambiati attraverso algoritmi crittografici;
  - scambio delle chiavi con algoritmi a chiavi asimmetriche;
  - cifratura dei dati applicativi con algoritmi a chiave simmetrica;
  - algoritmi di hashing e firma digitale;
- Procedure e processi per la protezione delle informazioni (PR.IP): gestione dei certificati e delle chiavi, in conformità allo standard IEC 62351-9[30], per mezzo di una infrastruttura di gestione delle chiavi pubbliche per le funzioni di registrazione dei dispositivi, emissione, rinnovo e revoca dei certificati e validazione del loro stato di validità;

27 Cfr. nota 19.

28 IEC 62351-3, Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP. Available online: https://webstore.iec.ch/en/publication/68410 (access on 14 August 2024).

29 IEC 62351-4, Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives. Available online: https://webstore.iec.ch/en/publication/67350 (access on 14 August 2024).

30 IEC 62351-9, Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment. Available online: https://webstore.iec.ch/en/publication/66864 (access on 14 August 2024).

- Anomalie e eventi (DE.AE): monitoraggio della sicurezza a supporto di attività di diagnostica e audit.

A supporto dei requisiti di conformità e certificazione introdotti dalla Legge Perimetro, la Norma CEI-016[31] richiede che il CCI sia dotato delle seguenti certificazioni rilasciate da terze parti:

- UCA IEC 61850 che attesti la conformità del profilo CCI allo standard IEC 61850;
- IEC 62351-100-3[32] che attesti la conformità del profilo di sicurezza di livello trasporto allo standard IEC 62351-3[33]. I test specificati includono verifiche sulla dimensione di chiavi e certificati, sui limiti temporali delle procedure di rinnovo e validità, test di comportamenti attesi e anomali (Figura 4);

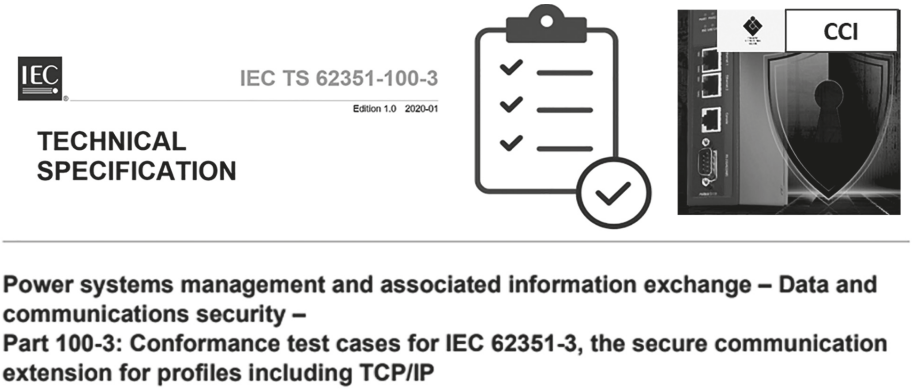


Figura 4 – Casi di Test per la conformità allo standard IEC 62351-3

- ISA/IEC 62443-4-1[34] che attesti la conformità del processo di sviluppo del CCI con livello di maturità 3;
- ISA/IEC 62443-4-2[35] che attesti i requisiti di sicurezza del dispositivo CCI con i livelli di sicurezza specificati in Figura 5;

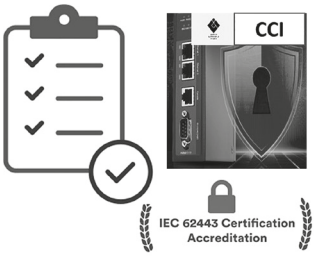
31 Cfr. nota 4.

32 IEC TS 62351-100-3, Power systems management and associated information exchange – Data and communications security – Part 100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP. Available online: https://webstore.iec.ch/en/publication/61597 (access on 14 August 2024).

33 Cfr. nota 21.

34 Cfr. nota 6.

35 Cfr. nota 7.



Foundational Requirement	Description	Security Level
FR1	Identification and authentication control(IAC)	2
FR2	Use control (UC)	2
FR3	System integrity (SI)	2
FR4	Data confidentiality (DC)	1
FR5	Restricted data flow (RDF)	1
FR6	Timely response to events (TRE)	1
FR7	Resource availability (RA)	3

Figura 5 – Certificazione ISA/IEC 62443

- FIPS 140-2 che attesti un grado di resistenza a manomissioni fisiche di livello 3 per il modulo di sicurezza hardware in cui sono memorizzate le chiavi crittografiche e i certificati elettronici.
- Nell'ambito del progetto 2.1 "Cybersecurity dei sistemi energetici" del Piano Triennale 22-24 della Ricerca di Sistema i profili di sicurezza della CEI 0-16 sono oggetto di test prestazionali[36] e di conformità[37]. Gli schemi di certificazione ISA/IEC 62443 vengono valutati in relazione ai test richiesti dal Centro di Valutazione e Certificazione Nazionale dell'ACN in ottemperanza alla Legge Perimetro.

5. Conclusioni

Il presente articolo ha illustrato, attraverso un ambito applicativo relativo alla digitalizzazione del settore energetico, il recepimento dei requisiti legislativi dei sistemi che ricadono nel perimetro di sicurezza nazionale cibernetica attraverso soluzioni di cybersecurity conformi a standard internazionali di settore.

Le esperienze pionieristiche riportate nell'articolo, oggetto di diverse azioni di divulgazione nazionale[38] ed internazionale[39], costituiscono una base di competenze utile per le numerose future applicazioni digitali in ambito energetico.

Affinché la transizione energetica delineata dal PNIEC[40] possa indirizzare l'autonomia tecnologica auspicata dalla strategia dell'Agenzia per la Cybersicurezza Nazionale risulta essenziale seguire il processo di recepimento nazionale della Direttiva NIS2 e l'evoluzione degli standard internazionali sviluppati dai comitati di riferimento.

36 Todeschini 2023.
37 Todeschini, Guagliardi 2023.
38 Dondossola, Terruggia, Todeschini, Bianco, Modica 2022.
39 Dondossola, Terruggia, Todeschini, Bianco, Delli Carpini, Modica 2024.
40 Cfr. nota 3.

Bibliografia

Dondossola G., Terruggia R., Todeschini M., Bianco G., Delli Carpini L., Modica M. 2024, "Cybersecurity-Enabling Technologies: Digital Applications" in *the Energy Transition, IEEE Power and Energy Magazine*, Volume: 22, Issue: 3, May-June, available online: https://ieeexplore.ieee.org/document/10522091?source=authoralert (access on 14 August 2024).

Dondossola G., Terruggia R., Todeschini M., Bianco G., Modica M. 2022, "L'implementazione della cybersecurity per lo scambio dati con utenti attivi MT", in *Rivista AEIT L'Energia Elettrica*, N. 2 Vol. 99, pagg 11-19, disponibile online: https://www.rse-web.it/pubblicazioni/limplementazione-della-cybersecurity-per-lo-scambio-dati-con-utenti-attivi-mt/ (accesso 14 Agosto 2024).

Todeschini M. 2023, "Progetto di un'architettura per la misurazione dell'impatto dell'autenticazione basata su PKI centralizzata nelle comunicazioni di telecontrollo", in *Ricerca di Sistema*, RSE n. 23006655.

Todeschini M. G., Guagliardi A. 2023, "Progettazione di una piattaforma automatizzata per test di conformità ai requisiti di cybersecurity delle comunicazioni nei dispositivi energetici", in *Ricerca di Sistema*, RSE n. 23006657.

Niloofar Kazemargi, Federica Ceci

Data Governance for Creating Value in Data Ecosystems

Abstract: In the present work we review the literature on data ecosystems to expand the current understanding of data governance. We discuss how data ecosystem governance involves coordination among different actors regarding data, data activities and data realms. The presence of various actors, responsible and accountable for data along the data value chain, create complexity and interdependencies. Our argument serves as a basis for both practitioners and academics to rethink data ecosystem governance by offering insights into the dynamics of data ecosystems and ensuring that these ecosystems effectively create value from data.

Keywords: Data Ecosystem; Data Governance; Data Activities; Actors; Governance Mechanisms.

1. Introduction

In the contemporary digital landscape, data stands as a pivotal asset driving innovation, strategic decision-making, and economic growth across various sectors. As a single organization does not possess all the required capabilities and resources to create, collect, store, integrate, exchange, and process data, thus, there is an inherent reliance on other organizations' capabilities and resources (Oliveira and Lóscio 2018). This leads to inter-organizational data collaborations and the emergence of complex socio-technical networks around data known as data ecosystems (Basole 2020; Oliveira et al. 2019). The formation of data ecosystems in different industrial sectors and countries presents organizations with new challenges, especially in mitigating risks associated with data collaboration while enhancing the value of data. Despite the fact that the literature emphasizes the importance of procedures and controls to mitigate risk associated with data activities at the organizational level, little is known about how data activities at the ecosystem level need to be governed.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760160

Prior research reveals similarities and differences between governance at organizational and ecosystem levels (Scholz et al. 2022). Although the literature provides insights about data ecosystem governance, does not adequately address the inherent complexity and dynamics of data ecosystems.

This paper aims to advance the understanding of data ecosystem governance by shifting the focus towards data as digital artifacts and examining the data value chain to illustrate the distributed nature of data and its integration with various technologies and actors. Through a literature review, we explore the nuances of coordinating governance across different data realms and among diverse stakeholders within the ecosystem. Our goal is to expand our understanding by reflecting on the intricacies of data ecosystem governance and providing actionable insights for effective management of data in a collaborative environment.

The paper is organized as follows: the next section provides a overview of existing knowledge and frameworks relevant to data ecosystems and governance. Following the theoretical framework, the paper details the methodological approach employed in the study. The fourth section engages in a critical analysis of the current paradigms of data governance. It challenges existing models and proposes new perspectives to better accommodate the complexities and dynamism of modern data ecosystems. The concluding section synthesizes the findings from the discussion and exploration stages, drawing conclusions about the state of data ecosystem governance and its implications for both theoretical frameworks and practical applications.

2. Theoretical Background

2.1. Data Ecosystems

Data ecosystems are defined as "socio-technical complex networks in which actors interact and collaborate with each other to find, archive, publish, consume, or reuse data as well as to foster innovation, create value, and support new businesses"(Oliveira et al. 2019, p. 590). Data ecosystems create value by having one group of actors produce or provide data while other actors within the ecosystem consume it (Janssen et al. 2012).

The literature categorizes data ecosystems based on the governance structure as market, hierarchy, network and bazaar (Lis and Otto 2021). Data ecosystems can have different degrees of openness. In open data ecosystems, any actor can join the ecosystem and use data with no constraint. The primary goal of an open data ecosystem is to enhance transparency and support decision-making. Contrary, in closed data ecosystems, only certain actors have permission to access and use the data (Gelhaar et al. 2021; Janssen et al. 2012). Another distinction can be made based on infrastructure. Data ecosystems can rely on proprietary infrastructure managed and owned by an actor – for instance, social media platforms (Alaimo et al. 2019) – or on distributed infrastructure to store, process and exchange data (Gelhaar and Otto 2020).

2.2. Data Governance

Data Governance is defined as "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what ac-tions with what information, and when, under what circumstances, using what methods"[1]. Literature on data governance focuses on the allocation of decision rights and the deployment of mechanisms to ensure the alignment of activities with organizational goals (Khatri and Brown 2010). Literature suggests different frameworks to ensure that data decisions are aligned with goals and objectives (Gregory et al. 2018; Tiwana et al. 2013) by identifying different roles within an organization (Abraham et al. 2019; Khatri and Brown 2010); for example, data governance leader, data owner, data producer, and the data consumer to name a few (Abraham et al. 2019; Jarvenpaa and Essén 2023).

The existing literature on data governance has mainly focused on the organizational level (Abraham et al. 2019): how an enterprise handles and uses its organizational assets. However, recently, scholars have seen a need for shifting the focus from the organizational to the ecosystem level as organizations increasingly rely on sharing and accessing data both within and outside the organizational boundaries (Abraham et al. 2019; Jagals and Karger 2021). The current frameworks although provide insights about data governance in inter-organizational context, do not fully address the challenges, complexity and dynamics that emerged from data collaboration and interactions of heterogeneous ecosystem actors (Lis and Otto 2020). Only recently, Micheli et al. (2020) empirically investigated and compared governance mechanisms among different data ecosystems.

Another research stream views data like other digital artifacts with peculiar characteristics and has ex-panded our understanding of data governance. For instance, Parmiggiani and Grisot (Parmiggiani and Grisot 2020) describe the importance of bottom-up decisions (rather than top-down) and the role of actors who actually work with data for data governance at the level. However, we know little about how data nature shapes data governance at the ecosystem level.

2.3. Data Value Chain

The Data Value Chain (DVC) outlines the progression of data from its initial collection to analysis, dissemination, and its ultimate influence on decision-making processes (Watch 2018). The concept organizes an organization's fundamental value-adding activities, enhancing understanding and optimization opportunities. A value chain comprises various subsystems, each involving inputs, transformation processes, and outputs. Rayport and Sviokla (1995)

1 https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/.

were pioneers in applying the value chain concept to information systems in their 1995 work on Virtual Value Chains. Integrating DVC within a smart environment enhances the performance of firms that recognize the critical importance of data (Mayhew et al. 2016). The DVC process, involves five stages (Cavanillas et al. 2016): data acquisition: this involves collecting, filtering, and cleaning data to produce an analyzable element for the data warehouse; data analysis: this stage includes exploring, transforming, and modeling data to render it strategically useful; data curation: this involves managing data to ensure it maintains the necessary quality throughout its lifecycle (Pennock 2007); data storage: data are efficiently grouped and stored in a scalable manner to facilitate quick and efficient access by relevant parties; data usage: this activity integrates data analysis into business processes through tools that support both the analysis and access to stored data.

The DVC is designed to model high-level activities within information systems, featuring more inter-connections than traditional value chains, and is central to the Data Ecosystem at a micro level, with numerous stakeholders at both meso and macro levels (Curry 2016). Contributions by Knabke & Olbrich (2015) and Mikalef & Gupta (2021) emphasize the role of dynamic capabilities in enhancing business intelligence and value, thereby enriching academic perspectives on how firms can adapt their roles and positions within the evolving big data and business analytics ecosystems. A robust analytics capability is essential for digital transformation, requiring organizations competing in the digital economy to invest in diverse resources such as personnel, processes, technologies, and organizational structure.

3. Research Method

The goal of the study is to develop a conceptual model for data ecosystem governance. To develop a conceptual model, we conducted a literature review (Webster and Watson 2002) of research on data governance and ecosystems. To identify relevant literature, we used AIS Electronic Library database for the searching phase. For key-based search, we used "data ecosystem*" as a keyword. Our analy-sis focused on governance in data ecosystems rather than data/information governance to ensure that our literature review provides new insights and expands the work of Abraham et al. (Abraham et al. 2019) and Scholz et al. (Scholz et al. 2022).

We conducted key-based search in May 2023. We also included peer-reviewed conference papers. In qualitative assessment, based on their titles and abstracts, we excluded articles that did not focus explicitly or implicitly on data governance or decisions about data management in data ecosystems. We also performed a forward and backward search to identify other relevant articles. In total, we reached 40 articles addressing data ecosystem governance.

During the analysis of the literature, key themes have emerged to delineate the focus of scholarly research on data, collectively enhancing our understand-

ing of different aspects of data governance. These themes include: (i) the concept of data as digital artifacts, (ii) the distribution of data tasks across various organizations, and (iii) the comprehensive areas encompassed by data realms. Specifically, these realms cover data quality, data value, data security and privacy, regulatory compliance, and data sustainability. Each of these components plays a crucial role in shaping the frameworks and strategies that govern the effective management and utilization of data in diverse contexts and they will be discussed in the next sections.

4. Discussion of results: Rethinking data ecosystem governance

With the formation and emergence of new data ecosystems, previous studies illustrate challenges in data governance regarding data rights, ownership, coordination, and incentive systems (Lis and Otto 2020; Susha et al. 2017). To show the complexity and dynamics of data ecosystems, we draw on the literature on digital artifacts and data value chain. This allows us to extend the scope of data governance by considering data not as organizational assets but as data objects (Kallinikos et al. 2013) which flow continuously across organizational and technological arrangements.

4.1. Data as Digital Artifacts

Data sources range from operational data, proprietary data, machine-generated data, user data on social media, open data to personal data. Data sources can be internal or external. Enterprise resource planning (ERP) systems, transactions, and organizational processes are some examples of internal data. External data are generated and aggregated outside of organizational boundaries such as third parties, user data and open data sources to name a few (Günther et al. 2017; Zuboff 2015).

The value of data changes over time (Pigni et al. 2016). Real-time data offers insights about instant events, allowing for agile decision-making (Pigni et al. 2016). Historical data are collected and stored over a longer period and are often used for trend analysis and strategic planning. Organizations can reuse data multiple times without data being consumed for different purposes (Constantiou and Kallinikos 2015; Günther et al. 2022; Newell and Marabelli 2015), due to their non-rival nature (Krämer 2020). Organizations use different types of data to draw insights from, ranging from raw data to data products (Hasan and Legner 2023). Data products are defined as "a managed artifact that satisfies recurring information needs and creates value through transforming and packaging relevant data elements into consumable form" (Hasan and Legner 2023). Data as other digital objects are self-referential (Kallinikos et al. 2013; Yoo et al. 2010). Consequently, data must use other digital technologies to create new insights from data. In other words, data creation, collection, storage, exchange, and process require digital technologies. For instance, a firm can use

data generated by users of its online services by relying on cloud services. Such technologies can be proprietary infrastructure managed and owned by an actor – for instance, social media platforms (Alaimo et al. 2019) – or distributed infrastructure to store, process and exchange data (Gelhaar and Otto 2020). A single actor may not necessarily possess all technologies (such as software and infrastructure) and thus relies on other actors' resources and capabilities for data processing and exchange (Assunção et al. 2015). Putting all these unique characteristics of data together, we need to expand the scope of data governance. First, to (re)combine data efficiently and effectively, data governance needs to focus on data formats and protocols to ensure the interoperability of data across different infrastructures. Data ecosystems could deploy guidelines and a shared framework (Kazemargi et al. 2023) specifying how data is to be shared in order to data facilitate data combination and (re)use.

Second, for data ecosystems to function and be sustained, data must be reused by different ecosystem actors. The ability to reuse data depends heavily on data governance. Data governance needs to control for what purposes data are used. In particular, data ecosystem governance involves defining policies and rules to determine what reuse purposes will be allowed in the ecosystem.

Third, controlling data resources needs to be another scope of data ecosystem governance. Since data flow across organizational boundaries and infrastructures, what infrastructures and applications are used for data creation, collection, storage, exchange, and processing data become relevant for data ecosystem governance.

4.2. Distributed Data Tasks

Considering the characteristics of digital data, organizations need to continuously make decisions around data access, data storage, data analysis for data-driven business models (Lange et al. 2021). This expands the scope of data ecosystem governance to include not only data as digital artifacts but also the alignment of data tasks with the overall strategy. For instance, decisions about revealing corporate data as open data (Enders et al. 2020) need to be aligned with a long-term organizational strategy. At the organizational level, the aim is to maximize the benefit of open data for an organization while limiting the negative consequences of open data. Such decisions have direct implications for value creation within an ecosystem.

Data tasks are interrelated. Decisions about data collection, curation and consumption (Basole 2020; Chua et al. 2022) influence data collaboration and consequently data-driven innovation. For instance, Parmiggiani and Grisot (2020) show that decisions related to data production and use influence data quality and consequently value generated by data. Within an ecosystem, data tasks are distributed among a diverse set of actors. For instance, Basole (2020) outlines some data are curated by different actors with different expertise and interests (e.g., crowd). Thus, data ecosystem governance should be seen as the effort to ensure the interests of the key stakeholders who own, provide and control plat-

forms and technology (2019), but also as the efforts to coordinate a diverse set of actors who use and share data. This is consistent with the work by Janssen et al. (2012) who argue that sustaining data ecosystems depends on the motivation and engagement of not only data providers but also data users.

Data ecosystem governance also should include not only what data to govern but also the data value chain: how data are created, collected, stored, exchanged, integrated, and processed. Governance over data tasks limits behavioral complexity, promotes fair use of data as collective resources, and addresses tensions among actors (van den Broek and van Veenstra 2018) to facilitate and promote data shar-ing (Lis and Otto 2021).

Previous studies also discuss data ecosystem governance needs to address also incentive structure (Tiwana et al. 2013), how to provide a structure and incentive to promote the participation of (new) actors generating, collecting, using, and exchanging data (Heinz et al. 2022; De Prieëlle et al. 2020).

4.3. Data Realms

Data ecosystems play a crucial role in shaping the digital landscape, demanding effective governance to optimize their potential and mitigate inherent risks. Within these ecosystems, several key elements – data quality, value, security, regulatory compliance, and sustainability – emerge as fundamental to their successful operation. High-quality data fuel accurate insights and superior decision-making, while the management of data security and privacy safeguards against potential violations and enhances trust among participants. Moreover, navigating the varying regulatory landscapes across different jurisdictions poses significant challenges, necessitating adaptive governance strategies that ensure compliance and facilitate long-term sustainability. As these ecosystems evolve, the need to balance diverse stakeholder interests, uphold data sovereignty, and sustainably manage data resources becomes ever more critical. This interplay of factors underpins the overarching frameworks and strategies that govern data ecosystems, ultimately influencing their efficacy and value generation. A description of the key elements follows:

Data Quality. Data quality influences the value that can be extracted from it: high-quality data enable more accurate insights and better decision-making. Data quality includes the integrity of data that organizations generate, collect, integrate, or curate (Basole 2020). In particular, evaluating the quality of open data is particularly important to ensure its accuracy and usefulness for various actors in a data ecosystem (Najafabadi and Cronemberger 2022). Evaluation of the quality of data requires a set of definitions, standards, and rules. While some organizations have adopted the organizational level standards, in data ecosystems, shared standards are needed. In the lack of shared standards for data quality, data ecosystems face the challenge of managing different data quality standards (Jarvenpaa and Essén 2023).

Data Value. Data ecosystem governance needs to address the interests and expectations of a diverse set of ecosystem actors (Lee et al. 2017; Scholz et al.

2022). This is a challenging task as these interests and expectations often differ and can sometimes conflict (Lauf et al. 2022). To sustain data ecosystems, data governance frameworks must incorporate data sovereignty[2], allowing stakeholders to negotiate and control the use of their data (Jarke et al. 2019). Another challenge in creating a sustainable data ecosystem is to ensure that all actors capture value, especially data owners. Thus, governance and the business model of data ecosystems are interrelated concepts.

Data Security/ Privacy. Enders et al. (2020) studied decisions related to data sharing and risks associated with releasing open data. Beyond carefully analyzing competitiveness and innovation opportunities, data security and privacy issues surface within data ecosystems as how one actor handles data may lead to a security/ privacy violation for other actors (Davidson et al. 2023; Newell and Marabelli 2015; Vial 2019)digital data are captured through a variety of devices that have the ability to monitor the minutiae of an individual's everyday life. These data are often processed by algorithms, which support (or drive. Thus, data ecosystems use a diverse set of governance mechanisms to mitigate security and privacy risks: for example guidelines, standards, contracts and bilateral agreements (Burmeister et al. 2021).

Regulatory Compliance. Data and data resources are managed by dispersed actors across industries and countries with different regulatory landscapes. In sectors with lax regulatory enforcement, regulatory compliance and norms are minimal, whereas highly regulated sectors require more adhesion to national and international regulations (Martin et al. 2019). Given the the complexity and evolution of the regulations coming into force, data ecosystem governance should therefore be aware of this and aim to resolve it (Kazemargi et al. 2023).

Data Sustainability. Deriving insights from historical and/or (re)combined data over time has given rise to data sustainability discussion. Data sustainability refers to the capacity to "data accumulation in the past and present is used to meet the needs of the present generation but without compromising the data's use in the future by heterogeneous, independent, and unknown actors" (Jarvenpaa and Essén 2023, p. 100449). Given the evolving technological and social arrangements, data sustainability is a crucial aspect of data ecosystem governance to ensure value creation in the long term by reusing and recombining data.

Conclusion

This study focused on the dynamics and the governance frameworks within data ecosystems. By embracing a perspective that views data not merely as organiza-

2 Data sovereignty refers to "the complete control over stored and processed data and the decision on who is permitted to have access to it". According to GAIA-X: Driver of digital innovation in Europe (2020).

tional assets but as dynamic digital artifacts that continuously interact across various boundaries, we uncover the complexity in data management and governance at the ecosystem level. Our research underscores the critical role of integrated data governance frameworks that align with the evolving nature of data ecosystems, marked by diverse actors and technologies.

Our contributions emphasize the importance of redefining data governance to encompass broader scopes – focusing not only on data protection and privacy but also on the strategic utilization of data through the data value chain. The proposed governance frameworks need to account for the continuous flow and reuse of data, ensuring interoperability, security, and sustainability. Such frameworks should also foster collaboration among ecosystem actors while balancing individual and collective goals, addressing inherent conflicts, and enhancing transparency and accountability. Moreover, by emphasizing the role of data as digital artifacts, the paper provides a novel perspective on how data is managed and utilized across different stages – from collection to usage. This integration can highlight the interconnectedness of data management processes and offer a holistic view that is often lacking in traditional data governance frameworks. This approach may lead to the development of more comprehensive governance strategies that address both the technical and organizational aspects of data ecosystems.

On a final note, by rethinking governance in light of the distributed nature of data and the multitude of actors involved, the paper emphasizes the importance of better coordination, transparency, and efficiency of data sharing and utilization. This is pivotal in managing the inherent risks and maximizing the value derived from data ecosystems. As data ecosystems continue to emerge and grow in complexity and significance, the insights derived from this study could serve as foundational guidelines for policymakers, industry leaders, and researchers. Future work should explore practical applications of these governance models in real-world settings and their impacts on innovation, efficiency, and the equitable distribution of data-driven benefits. This will not only refine theoretical models but also ensure that data ecosystems are leveraged effectively to foster sustainable growth and innovation across sectors.

Acknowledgments: Finanziato dall'Unione europea – Next Generation EU, Missione 4 Componente 2, PRIN 2022 PNRR, CUPD53D23017780001, Titolo del progettoL "Data4Innovation – Data ecosystem governance toward enhancing data sharing for innovation: implications for organizations"

References

Abraham, R., Schneider, J., and vom Brocke, J. 2019. "Data Governance: A Conceptual Framework, Structured Review, and Research Agenda", in *International Journal of Information Management* (49:July), Elsevier, pp. 424-438. (https://doi.org/10.1016/j.ijinfomgt.2019.07.008).

Alaimo, C., Kallinikos, J., and Valderrama, E. 2019. "Platforms as Service Ecosystems: Lessons from Social Media", in *Journal of Information Technology*. (https://doi.org/10.1177/0268396219881462).

Assunção, M. D., Calheiros, R. N., Bianchi, S., Netto, M. A. S., and Buyya, R. 2015. "Big Data Computing and Clouds: Trends and Future Directions", in *Journal of Parallel and Distributed Computing* (79), Elsevier, pp. 3-15.

Basole, R. C. 2020. "Understanding Ecosystem Data", in *Proceedings of the Annual Hawaii International Conference on System Sciences* (2020-Janua), pp. 5718-5727. (https://doi.org/10.24251/hicss.2020.702).

Burmeister, F., Kurtz, C., Vogel, P., Drews, P., Schirmer, I., Burmeister, F., Vogel, P., Kurtz, C., Drews, P., and Schirmer, I. 2021. "Unraveling Privacy Concerns in Complex Data Ecosystems with Architectural Thinking," in *ICIS 2021 Proceedings*.

Cavanillas, J. M., Curry, E., and Wahlster, W. 2016. *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*, Springer Nature.

Chua, C., Indulska, M., Lukyanenko, R., Montr, H. E. C., Maass, W., and Storey, V. C. 2022. *MISQ Research Curation on Data Management Research*, pp. 1-12.

Constantiou, I. D., and Kallinikos, J. 2015. "New Games, New Rules: Big Data and the Changing Context of Strategy," *Journal of Information Technology* (30:1), pp. 44-57. (https://doi.org/10.1057/jit.2014.17).

Curry, E. 2016. "The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches," *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*, Springer International Publishing, pp. 29-37.

Davidson, E., Wessel, L., Winter, J. S., and Winter, S. 2023. "Future Directions for Scholarship on Data Governance, Digital Innovation, and Grand Challenges," *Information and Organization* (33:1), Elsevier Ltd, p. 100454. (https://doi.org/10.1016/j.infoandorg.2023.100454).

De Prieëlle, F., De Reuver, M., and Rezaei, J. 2020. "The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry," *IEEE Transactions on Engineering Management*, IEEE.

Enders, T., Wolff, C., and Satzger, G. 2020. "Knowing What to Share: Selective Revealing in Open Data," *ECIS 2020 – Proceedings of the 28th European Conference on Information Systems*.

Gelhaar, J., Groß, T., and Otto, B. 2021. "A Taxonomy for Data Ecosystems," *Proceedings of the Annual Hawaii International Conference on System Sciences* (2020-Janua), pp. 6113-6122. (https://doi.org/10.24251/hicss.2021.739).

Gelhaar, J., and Otto, B. 2020. "Challenges in the Emergence of Data Ecosystems," *Proceedings of the 24th Pacific Asia Conference on Information Systems*.

Gregory, R. W., Kaganer, E., Henfridsson, O., and Ruch, T. J. 2018. *IT Consumerization and the Transformation of IT Governance*, (42:4), pp. 1225-1253. (https://doi.org/10.25300/MISQ/2018/13703).

Günther, W. A., Rezazade Mehrizi, M. H., Huysman, M., Deken, F., and Feldberg, F. 2022. "Resourcing with Data: Unpacking the Process of Creating Data-Driven Value Propositions," *Journal of Strategic Information Systems* (31:4), Elsevier B.V., p. 101744. (https://doi.org/10.1016/j.jsis.2022.101744).

Günther, W. A., Rezazade Mehrizi, M. H., Huysman, M., and Feldberg, F. 2017. "Debating Big Data: A Literature Review on Realizing Value from Big Data," *Journal of Strategic Information Systems* (26:3), pp. 191-209. (https://doi.org/10.1016/j.jsis.2017.07.003).

Hasan, M. R., and Legner, C. 2023. "Understanding Data Products: Motivations, Definition, and Categories and Categories," *Ecis*, pp. 5-11. (https://aisel.aisnet.org/ecis2023_rp/229).

Heinz, D., Benz, C., Fassnacht, M., and Satzger, G. 2022. "Past, Present and Future of Data Ecosystems Research: A Systematic Literature Review," *PACIS 2022 Proceedings*. (https://aisel.aisnet.org/pacis2022).

Jagals, M., and Karger, E. 2021. "Inter-Organisational Data Governance: A Literature Review," *ECIS 2021 Research Papers* (June), pp. 1-19. (https://aisel.aisnet.org/ecis2021_rp/57).

Janssen, M., Charalabidis, Y., and Zuiderwijk, A. 2012. "Benefits, Adoption Barriers and Myths of Open Data and Open Government," *Information Systems Management* (29:4), pp. 258-268.

Jarke, M., Otto, B., and Ram, S. 2019. "Data Sovereignty and Data Space Ecosystems," *Business and Information Systems Engineering* (61:5), Springer Fachmedien Wiesbaden, pp. 549-550. (https://doi.org/10.1007/s12599-019-00614-2).

Jarvenpaa, S. L., and Essén, A. 2023. "Data Sustainability: Data Governance in Data Infrastructures across Technological and Human Generations," *Information and Organization* (33:1). (https://doi.org/10.1016/j.infoandorg.2023.100449).

Kallinikos, J., Aaltonen, A., and Marton, A. 2013. "THE AMBIVALENT ONTOLOGY OF DIGITAL ARTIFACTS," *MIS Quarterly* (37:2), pp. 357-370.

Kazemargi, N., Spagnoletti, P., Constantinides, P., and Prencipe, A. 2023. "Data Control Coordination in Cloud-Based Ecosystems: The EU GAIA-X Ecosystem," in *Research Handbook on Digital Strategy*, & F. Z. C. Cennamo, G. B. Dagnino (ed.), Edward Elgar Publishing, pp. 289-307. (https://doi.org/10.4337/9781800378902.00024).

Khatri, V., and Brown, C. V. 2010. "Designing Data Governance," *Communications of the ACM* (53:1), pp. 148-152. (https://doi.org/10.1145/1629175.1629210).

Knabke, T., and Olbrich, S. 2015. *Exploring the Future Shape of Business Intelligence: Mapping Dynamic Capabilities of Information Systems to Business Intelligence Agility*.

Krämer, J. 2020. "Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations," *Journal of Competition Law & Economics* (17:2), pp. 263-308. (https://doi.org/10.1093/joclec/nhaa030).

Lange, H. E., Drews, P., and Höft, M. 2021. "Realization of Data-Driven Business Models in Incumbent Companies: An Exploratory Study Based on the Resource-Based View," *ICIS 2021 Proceedings*, pp. 1-17.

Lauf, F., Scheider, S., and Bartsch, J. 2022. "Linking Data Sovereignty and Data Economy : Arising Areas of Tension," in *Wirtschaftsinformatik 2022 Proceedings*.

Lee, S. U., Zhu, L., and Jeffery, R. 2017. "Data Governance for Platform Ecosystems: Critical Factors and the State of Practice," in *Pacific Asia Conference on Information Systems*.

Lis, D., and Otto, B. 2020. "Data Governance in Data Ecosystems – Insights from Organizations," in *AMCIS 2020 Proceedings.*

Lis, D., and Otto, B. 2021. "Towards a Taxonomy of Ecosystem Data Governance," *Proceedings of the Annual Hawaii International Conference on System Sciences* (2020-Janua), pp. 6067-6076. (https://doi.org/10.24251/hicss.2021.733).

Martin, N., Matt, C., Niebel, C., and Blind, K. 2019. "How Data Protection Regulation Affects Startup Innovation," *Information Systems Frontiers* (21:6), Information Systems Frontiers, pp. 1307-1324. (https://doi.org/10.1007/s10796-019-09974-2).

Mayhew, H., Saleh, T., and Williams, S. 2016. "Making Data Analytics Work for You—Instead of the Other Way Around," *McKinsey Quarterly* (4), pp. 1-8.

Micheli, M., Ponti, M., Craglia, M., and Berti Suman, A. 2020. "Emerging Models of Data Governance in the Age of Datafication," *Big Data and Society* (7:2). (https://doi.org/10.1177/2053951720948087).

Mikalef, P., and Gupta, M. 2021. "Artificial Intelligence Capability: Conceptualization, Measurement Calibration, and Empirical Study on Its Impact on Organizational Creativity and Firm Performance," *Information and Management* (58:3), Elsevier B.V., p. 103434. (https://doi.org/10.1016/j.im.2021.103434).

Najafabadi, M. M., and Cronemberger, F. A. 2022. "Systemic Effects of an Open Government Program on Data Quality: The Case of the New York State's Food Protection Program Area," *Transforming Government: People, Process and Policy*. (https://doi.org/10.1108/TG-11-2021-0194).

Newell, S., and Marabelli, M. 2015. "Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of 'Datification,'" *Journal of Strategic Information Systems* (24:1), Elsevier B.V., pp. 3-14. (https://doi.org/10.1016/j.jsis.2015.02.001).

Oliveira, M. I. S., and Lóscio, B. F. 2018. "What Is a Data Ecosystem?," *ACM International Conference Proceeding Series*. (https://doi.org/10.1145/3209281.3209335).

Oliveira, M. I. S., Lóscio, B. F., and Lima, G. de F. B. 2019. "Investigations into Data Ecosystems: A Systematic Mapping Study," *Knowledge and Information Systems* (Vol. 61), Springer London. (https://doi.org/10.1007/s10115-018-1323-6).

Otto, B., and Jarke, M. 2019. "Designing a Multi-Sided Data Platform: Findings from the International Data Spaces Case," *Electronic Markets* (29:4), pp. 561-580. (https://doi.org/10.1007/s12525-019-00362-x).

Parmiggiani, E., and Grisot, M. 2020. "Data Curation as Governance Practice," *Scandinavian Journal of Information Systems* (32:1), pp. 1-38.

Pennock, M. 2007. "Digital Curation: A Life-Cycle Approach to Managing and Preserving Usable Digital Information," *Library & Archives* (1:1), n, pp. 1-3.

Pigni, F., Piccoli, G., and Watson, R. 2016. "Digital Data Streams: Creating Value from the Real-Time Flow of Big Data," *California Management Review* (58:3), pp. 5-25. (https://doi.org/10.1525/cmr.2016.58.3.5).

Rayport, J. F., & Sviokla, J. J. 1995. "Exploiting the Virtual Value Chain," *Harward Review., Buisness*, Boston.

Scholz, N., Wieland, J., and Schäffer, T. 2022. "Towards a Framework for Enterprise & Platform Ecosystem Data," in *AMCIS 2022 Proceedings*.

Susha, I., Janssen, M., and Verhulst, S. 2017. "Data Collaboratives as a New Frontier of Cross-Sector Partnerships in the Age of Open Data: Taxonomy Development," *Proceedings of the Annual Hawaii International Conference on System Sciences* (2017-Janua), pp. 2691-2700. (https://doi.org/10.24251/hicss.2017.325).

Tiwana, A., Konsynski, B., and Venkatraman, N. 2013. "Information Technology and Organizational Governance: The IT Governance Cube," *Journal of Management Information Systems* (30:3), Taylor & Francis, pp. 7-12.

van den Broek, T., and van Veenstra, A. F. 2018. "Governance of Big Data Collaborations: How to Balance Regulatory Compliance and Disruptive Innovation," *Technological Forecasting and Social Change* (129), Elsevier, pp. 330-338. (https://doi.org/10.1016/j.techfore.2017.09.040).

Vial, G. 2019. "Understanding Digital Transformation: A Review and a Research Agenda," *Journal of Strategic Information Systems* (28:2), Elsevier, pp. 118-144. (https://doi.org/10.1016/j.jsis.2019.01.003).

Watch, O. D. 2018. "The Data Value Chain: Moving from Production to Impact," *Data2X. Https://Opendatawatch. Com/Publications/the-Data-Value-Chain-Moving-from-pro Duction-to-Impact*.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, JSTOR, xiii–xxiii.

Yoo, Y., Henfridsson, O., and Lyytinen, K. 2010. "The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research," *Information Systems Research* (21:4), pp. 724-735. (https://doi.org/10.1287/isre.1100.0322).

Zuboff, S. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* (30:1), Springer, pp. 75-89.

Manfredi Matassa

Sicurezza cibernetica e nazionale nell'ordinamento multilivello: quale possibile convivenza?

Abstract: Il paper si concentra sul rapporto tra cybersecurity e sicurezza nazionale da una prospettiva funzionale, con l'obiettivo principale di individuare le problematiche della coesistenza di queste funzioni nel sistema multilivello. In particolare, dopo un inquadramento generale volto ad affrontare alcune questioni definitorie centrali ritenute indispensabili ai fini dell'analisi, l'elaborato intende evidenziare le ricadute del mutevole rapporto tra i concetti in esame. L'analisi mira ad approfondire il tema sia con riferimento alla distribuzione delle competenze tra Unione Europea e Stati membri (sul versante verticale) sia tra gli attori pubblici e privati coinvolti (sul versante orizzontale).

Keywords: Cybersecurity; Sicurezza nazionale; ENISA; Agenzia per la Cybersicurezza Nazionale; ACN.

1. Inquadramento del campo di indagine

Nel corso degli ultimi anni la sicurezza cibernetica[1] ha assunto una crescente centralità all'interno del dibattito giuspubblicistico fino al punto di assumere i caratteri di una inedita funzione pubblica distinta rispetto alle tradizionali funzioni di sicurezza. Partendo dal presupposto per cui l'esponenziale aumento delle capacità lesive degli attacchi informatici abbia elevato la cibersicurezza a prerequisito essenziale per la sopravvivenza di qualsiasi organizzazione complessa, la materia in oggetto si è ormai imposta al centro delle agende di ogni legislatore.

1 Al fine di prevenire equivoci di tipo terminologico si precisa che nel presente scritto le espressioni 'sicurezza cibernetica', 'sicurezza informatica' e 'cibersicurezza' – anche nella sua versione anglofona '*cybersecurity*' – saranno impiegati come sinonimi. Ritenendo condivisibili i rilievi mossi dall'Accademia della Crusca in tal senso, si è ritenuto opportuno non utilizzare la dicitura ibrida 'cybersicurezza' al momento preferita dal legislatore italiano. Per un inquadramento di ampio respiro sul tema si rinvia, tra gli altri, a Giupponi 2024: 277-303, Longo 2024: 313-347, Buoso 2023; Rossa 2023; Carotti 2020: 629-641; Serini 2022: 241-272; Ursi 2023: 7-20 e Matassa 2023: 21-42.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760161

L'Unione europea non è stata di certo tra le prime istituzioni ad acquisire una piena consapevolezza circa la necessità di adottare in tempi rapidi dei modelli regolatori capaci di affrontare al meglio le future sfide di sicurezza cibernetica[2]. Nonostante la *cybersecurity* si sia affermata come componente indispensabile soltanto in anni recenti, oggi non sorprende notare tra le prime venti posizioni del *Global Cybersecurity Index* la presenza di ben undici Paesi europei[3]. Ebbene, senza voler sminuire gli sforzi individuali compiuti dagli Stati tradizionalmente più attenti al tema della sicurezza informatica[4], i meriti riconosciuti a tali Paesi devono ritenersi in larga parte connessi ai recenti interventi europei che hanno permesso la realizzazione di un'infrastruttura comune di sicurezza cibernetica all'avanguardia.

Cionondimeno, il percorso che ha portato alla creazione dell'attuale architettura di difesa cibernetica europea è stato tutt'altro che lineare. La *cybersecurity* è stata catalogata nel novero degli '*important issues*' europei già in una raccomandazione del 2000, ma – stante l'istituzione nel 2004 di un'Agenzia temporanea preposta alla sicurezza della rete e delle informazioni (ENISA) e di altri interventi settoriali non particolarmente incisivi – il tema non è stato oggetto di vere e proprie iniziative regolamentari fino all'adozione della *Network and Information Security directive* ('direttiva NIS') del 2016. La pubblicazione di tale direttiva non è stato un punto di arrivo delle politiche europee di cibersicurezza, ma ha segnato l'inizio di una fase di iperproduzione normativa – ancora oggi *in itinere* – che ha dato vita a una disciplina straordinariamente complessa e intricata. Infatti, tra le fonti primarie a livello euro-unionale in materia di sicurezza cibernetica più rilevanti, oggi in vigore è possibile ricordare il regolamento 881/2019 ('cybersecurity Act'), il regolamento 2554/2022 ('regolamento DORA') e la direttiva 2555/2022 ('direttiva NIS II'). Inoltre, tale pacchetto normativo è destinato a essere ampliato nel prossimo futuro da due ulteriori pilastri regolatori, volti da un lato ad aggiornare il sistema di certificazioni di cibersicurezza ('Cyber Resilience Act') e, dall'altro, a istituire uno scudo di difesa europea basato su meccanismi solidali e incentivanti ('Cyber Solidarity Act').

L'approccio italiano alla sicurezza cibernetica si è distinto da quello degli altri Paesi europei per la sua struttura innovativa e articolata. Negli ultimi anni l'Italia

2 Ad esempio, gli Stati Uniti hanno inserito la *cybersecurity* tra le priorità del governo federale già nel 1997, dimostrando già allora consapevolezza circa l'importanza che avrebbe avuto il tema nel determinare i futuri equilibri tra Stati (mentre, come si avrà modo di evidenziare *infra*, la prima disciplina organica dell'Unione europea risale al 2016).

3 ITU, Global Cybersecurity Index (GCI) 2020, 25, reperibile su www.itu.int (visitato il 18 luglio 2024). Segnatamente, all'interno del '*global score and rank*' si segnalano, in ordine di apparizione: Estonia (3°), Spagna (4°), Lituania (6°), Francia (9°), Lussemburgo e Germania (13°), Portogallo (14°), Lettonia (15°), Olanda (16°), Belgio 19° e Italia (20°).

4 Tra gli esempi più virtuosi non possono che segnalarsi i differenti modelli di difesa cibernetica elaborati da Francia e Germania: la prima ha creato un'agenzia destinata alla sicurezza cibernetica (ANSSI) già nel 2008 durante la presidenza di Sarkozy; la seconda ha fondato nel 1991 (dunque ancor prima della stessa diffusione commerciale di Internet) il *Bundesamt für Sicherheit in der Informationstechnik* come autorità dedicato all'ufficio federale della sicurezza informatica.

ha intrapreso significativi passi avanti nel rafforzare le proprie capacità di difesa e risposta agli attacchi informatici attraverso l'elaborazione *ad hoc* di strumenti e apparati inediti volti a far fronte alle nuove sfide imposte dalla cibersicurezza. L'assoluta priorità acquisita dalla sicurezza cibernetica nell'agenda degli ultimi governi non è determinata esclusivamente dai nascenti obblighi di matrice euro-unitari, ma è stata stimolata anche (forse soprattutto) da fattori esogeni. Basti pensare che, dal primo semestre del 2018 al secondo semestre del 2023, è stato rilevato un aumento dell'86% degli attacchi informatici e nello stesso periodo la media di attacchi gravi per mese è passata da 124 a 230 (arrivando così a quasi otto per giorno)[5].

Nel conteso descritto, preso atto della circostanza per cui le organizzazioni pubbliche e private italiane fossero maggiormente esposte agli attacchi informatici rispetto alla media europea, il legislatore nazionale è stato chiamato ad affrontare il tema della sicurezza cibernetica attraverso l'elaborazione di soluzioni spesso originali. In particolare, come si avrà modo di approfondire *infra*, se in un primo momento il decisore politico italiano si è limitato a una mera attuazione delle misure contenute all'interno della direttiva NIS, dopo appena un anno l'architettura normativa nazionale si è distinta (in positivo) per aver introdotto uno strumento di sicurezza informatica all'avanguardia, ossia il Perimetro di Sicurezza Nazionale Cibernetica (d'ora in avanti 'PSNC' o 'Perimetro'). Peraltro, al di là degli obiettivi fissati dalla strategia quinquennale in materia di sicurezza cibernetica 2022-2026 e dal piano triennale per l'informatica della pubblica amministrazione 2024-2026, negli ultimi anni si è realizzato un complessivo ripensamento dell'intera infrastruttura di sicurezza cibernetica trainato soprattutto dall'istituzione dell'Agenzia per la Cybersicurezza Nazionale (d'ora in avanti 'ACN' o 'Agenzia'). In ultimo, oltre alla recentissima approvazione della l. 28 giugno 2024, n. 90 (dapprima noto come 'd.d.l. cyber'), il quadro normativo nazionale è destinato ad arricchirsi ulteriormente con la necessaria e attuazione della direttiva NIS2[6].

A un primo sguardo la componente nazionale di sicurezza cibernetica sembra collegata con quella europea fino al punto da risultare non tanto complementare, quanto piuttosto ricollegata a una medesima e inedita funzione dal carattere autonomo (ossia la sicurezza cibernetica). Cionondimeno, osservando con maggiore accortezza la disciplina descritta è possibile notare delle distinzioni profonde al punto da mettere in dubbio qualsiasi tentativo di *reductio ad unum* della materia. Nonostante sul piano concreto le 'dimensioni' della cibersicurezza tendano in larga parte a coincidere, occorre notare, come sul piano teorico, le stesse perseguano tra loro finalità ben distinte: il livello europeo della sicurezza cibernetica è volto

5 Clusit, *Rapporto 2024 sulla Sicurezza ICT in Italia*, 15 reperibile su https://clusit.it/rapporto-clusit (visitato il 12 ottobre 2024). Più nel dettaglio, i dati indicati nel rapporto mettono in evidenza come – al di là degli 'attacchi multipli' (19,4%) – il settore più colpito da tali attacchi è il settore sanitario con una percentuale che si assesta sul 14,3%, seguito da quello governativo e militare che si assesta sull'11,7%.

6 La direttiva NIS2 è stata da ultimo recepita nell'ordinamento italiano con il d.lgs. 4 settembre 2024, n. 138.

alla tutela del mercato interno dell'Unione, mentre quello italiano è indirizzato alla tutela della sicurezza nazionale.

Oltre a mettere in discussione qualsiasi lettura volta ad attribuire alla sicurezza cibernetica il carattere di funzione autonoma e unitaria, la distinzione in esame porta con sé delle conseguenze di ordine pratico. La scelta del legislatore italiano di ricondurre la *cybersecurity* nell'alveo della sicurezza nazionale permette di esercitare sulla parte della materia la 'riserva di Stato' di cui all'art. 4, par. 2, del Trattato sull'Unione europea (TUE), il quale, dopo aver individuato le 'funzioni essenziali dello Stato', precisa che "[…] la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro". Su tali presupposti, comprendere la relazione tra le funzioni di tutela del mercato e quelle di sicurezza nazionale si rivela essenziale per approfondire *in primis* i rapporti tra il versante nazionale ed europeo della materia e, *in secundis*, come immediata ricaduta, il grado di cedevolezza delle tutele dei privati rispetto all'interesse 'superiore' (supremo?) alla sicurezza. Cionondimeno, lo studio non potrebbe raggiungere gli obiettivi prefissati senza aver prima fornito alcune definizioni volte a permettere un corretto inquadramento generale della materia.

2. Alcuni necessari chiarimenti sul versante definitorio

Una delle principali cause che ha rallentato lo sviluppo di studi in campo pubblicistico volti ad approfondire il tema in oggetto può ricondursi alla possibilità di considerare ambedue le componenti essenziali poste alla base della nozione di *cybersecurity* (ossia la sicurezza e la cibernetica) dei 'concetti giuridici indeterminati'.

Nel diritto pubblico, così come nel linguaggio comune, la nozione di sicurezza può essere osservata soltanto dopo aver collocato il concetto in un determinato "paradigma"[7] o "dimensione"[8]. Così, partendo dall'assunto per cui la sicurezza è "un concetto generico e vuoto, che se non è specificato o riempito non significa nulla" (Bobbio 1976, 322), la scienza giuridica ha sviluppato dei metodi di indagine 'relazionali' utili ai fini dell'individuazione di nuovi significati della nozione. Tra questi è possibile distinguere gli approcci basati su una prospettiva relazionale 'in positivo' (volti cioè a ricercare il contenuto del termine mediante un raffronto con profili di valutazione di tipo oggettivo e soggettivo) dagli approcci volti a ricostruire il significato di sicurezza 'in negativo' (partendo dall'individuazione del rischio quale elemento speculare al concetto di sicurezza). Cionondimeno, poiché nella materia in esame la nozione di 'sicurezza' entra in contatto con un altro concetto giuridico indeterminato (la cibernetica), comprendere l'esatto significato del termine 'cibersicurezza' si dimostra un compito tutt'altro che agevole.

7 Per un approfondimento sull'evoluzione dei "paradigmi giuridici della sicurezza" in Italia si rimanda all'analisi di Ursi 2022: 15-46.

8 Sul punto si rimanda in generale al lavoro di Giupponi 2008: *passim*.

Poiché considerazioni in larga parte analoghe possono estendersi al concetto di 'sicurezza nazionale', considerato "giuridicamente evanescente" (Monti 2020, 75) nonché riconducibile alla sfera del "pre-, extra-, o meta-giuridico" (Barberis 2017, 97), in un simile scenario chiunque intenda approfondire la relazione tra le nozioni di sicurezza cibernetica e sicurezza nazionale è chiamato a misurarsi con ostacoli posti su più livelli. Non potendo in questa sede soffermarsi sui numerosi problemi di natura definitoria messi a fuoco dalla dottrina d'oltreoceano nel corso dell'ultimo ventennio, si ritiene opportuno evidenziare che, allo stato dell'arte, è possibile ricavare dalla normativa vigente una definizione di 'sicurezza cibernetica' ma non di 'sicurezza nazionale'.

Segnatamente, prendendo atto della coesistenza di almeno diciotto definizioni diverse di *cybersecurity* (Fuster e Jasmontaite 2020: 105-106), il legislatore europeo ha definito all'art. 2, comma 1, del regolamento 881/2019 la 'cibersicurezza' come "l'insieme delle attività necessarie per proteggere la rete e i servizi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche". Tale definizione è stata successivamente sviluppata nel diritto nazionale dall'art. 1, comma 1, lett. a) del d.l. 14 giugno 2021, n. 82, come "l'insieme delle attività […] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico"[9]. Ebbene, le modifiche apportate dal legislatore italiano alla definizione di cibersicurezza possono essere comprese soltanto se lette in combinato disposto con la nozione di 'resilienza nazionale nello spazio cibernetico', introdotta nella successiva lett. b), ossia "quel complesso di attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'art. 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131"[10].

Se sul versante formale la distinzione tra 'cybersicurezza' e 'resilienza nazionale nello spazio cibernetico' sembra collocare tali concetti in una relazione da genere a specie, non può ignorarsi come – in una prospettiva sostanziale (e più approfondita) – la normativa di riferimento si presti anche a interpretazioni differenti.

9 Ragioni di completezza di analisi suggeriscono di riportare per intero il contenuto del citato art. 1, comma 1, lett. a), d.l. 82/2021: "[ai fini del presente decreto si intende per 'cybersicurezza'] l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico".

10 Art. 1, comma 1, lett. f), DPCM 30 luglio 2020, n. 131: "[ai fini del presente decreto si intende per 'pregiudizio per la sicurezza nazionale'] danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero gli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale […]".

Difatti, inquadrando i concetti presi in esame in chiave formalistica, la sicurezza cibernetica potrebbe essere rappresentata come una nozione ampia al punto da ricomprendere al suo interno tutte quelle attività volte non solo ad assicurare la riservatezza, l'integrità e la disponibilità dei dati (la Triade nota come RID o CIA), ma anche la "sicurezza nazionale nello spazio cibernetico". Diversamente, la resilienza nazionale nel ciberspazio è un concetto legato a doppio filo con quello della tutela della sicurezza nazionale (e dunque riferito a una componente speciale di 'resilienza'). Una simile chiave di lettura potrebbe essere utilizzata quale fondamento teorico generale per individuare con sufficiente determinatezza un criterio distintivo tra le competenze in materia di sicurezza cibernetica, in astratto attribuibili all'Unione europea, e quelle necessariamente riservate agli Stati membri in forza dei limiti stabiliti dall'art. 4, par. 2, TUE.

Tuttavia, un'analisi più puntuale del quadro normativo nazionale permette di mettere in dubbio la possibilità di distinguere in modo chiaro questi concetti. Del resto, è sufficiente esaminare il contenuto del citato art. 1, comma 1, lett. f) del DPCM 131/2020 per notare come la nozione di 'sicurezza nazionale' non si presti a essere agevolmente contenuta all'interno di un perimetro circoscritto. Infatti, come già messo in evidenza *supra*, quest'ultimo termine è stato descritto dal legislatore in modo talmente ampio da ricomprendere non solo qualsiasi "danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche", ma anche qualsiasi pericolo ricollegato agli "interessi politici, militari, economici, scientifici e industriali dell'Italia". Ebbene, figurando la tutela della riservatezza, integrità e disponibilità dei dati tra gli 'interessi nazionali' politici ed economici, una lettura estensiva del combinato disposto permette di ricavare un significato del concetto di sicurezza cibernetica più ampio rispetto a quello attribuito alla sicurezza nazionale. Così, a seconda dell'angolo visuale, ognuno dei due concetti finisce per diventare allo stesso tempo sia contenuto, sia contenitore dell'altro.

Su tali premesse la scelta del legislatore nazionale di introdurre una (quantomeno equivoca) distinzione tra i concetti di 'sicurezza' e 'resilienza' cibernetica può ritenersi tutt'altro che casuale. *A contrario*, considerata anche la limitata utilità pratica della distinzione presa in esame, il parziale distacco rispetto alla definizione elaborata dal reg. (UE) 881/2019 può ritenersi frutto della volontà del decisore nazionale di mantenere intatti i benefici concessi dall'ambiguità del rapporto tra sicurezza cibernetica e sicurezza nazionale. Tale meccanismo permette alle istituzioni nazionali di valutare la medesima funzione talvolta come attività condivisa con l'Unione, consentendo così di beneficiare dei meccanismi di solidarietà europea (si pensi alla condivisione di informazioni e alla distribuzione di risorse vincolate al miglioramento dell'infrastruttura di difesa cibernetica nazionale), talvolta come attività strettamente correlata alla sicurezza nazionale. Ed infatti, il parallelismo tra sicurezza cibernetica e nazionale attribuisce alla Presidenza del Consiglio dei ministri – e all'ACN – poteri capaci di incidere sensibilmente sui diritti di libera iniziativa economica dei privati[11].

11 Assumono particolare rilievo in tal senso i poteri in materia di Perimetro Nazionale

3. La cibersicurezza come funzione tra sicurezza nazionale ed esigenze di tutela del mercato dell'Unione

Sulla base degli elementi fin qui tratteggiati la sicurezza cibernetica può essere rappresentata, almeno in una prima approssimazione, come una funzione pubblica complessa, multilivello, dal carattere composito e che coinvolge al suo interno due distinti gruppi di funzioni: uno strettamente collegato al paradigma securitario della materia (difesa, sicurezza pubblica, sicurezza nazionale e – più di recente – difesa attiva[12]) e un secondo a funzioni dal carattere spesso eterogeneo elaborate *ad hoc* per far fronte alle minacce cibernetiche, ossia quelle connesse alla tutela della 'Triade'(riservatezza, l'integrità e la disponibilità dei dati). Tuttavia, la relazione tra questi due gruppi di funzioni è cambiata radicalmente nel corso degli ultimi anni seguendo l'evoluzione del rapporto tra l'infrastruttura nazionale ed europea in materia di sicurezza cibernetica.

In una prima fase (2013-2021) il rapporto tra le esigenze di tutela del mercato interno e quelle della sicurezza nazionale si poteva inquadrare in un'ottica di completamento della disciplina nazionale rispetto a quella dell'Unione. Sul fronte europeo, la direttiva NIS si era occupata di disegnare una prima linea di difesa volta a offrire un livello di tutela al mercato interno dell'Unione (lasciando fuori dal campo di applicazione alcuni settori essenziali tra cui – oltre alla Pubblica Amministrazione – il settore nucleare e spaziale). Sul fronte nazionale, invece, la disciplina del 'decreto Perimetro' ha inteso dotare l'Italia di uno strumento diretto alla protezione in via autonoma di infrastrutture ritenute rilevanti per la sicurezza nazionale del Paese. Così, partendo dall'idea per cui nelle materie di 'sicurezza' il titolare di una funzione è il soggetto preposto a valutare il livello di rischio o di pericolo (lasciando l'individuazione del rischio o del pericolo in sé al decisore politico), fino al 2021 era possibile distinguere, almeno tendenzialmente, le funzioni esclusivamente statali volte a garantire la sicurezza nazionale da quelle condivise con l'Unione europea, nell'esercizio delle quali l'amministrazione nazionale agiva soprattutto 'in funzione comunitaria'[13]. Lo scenario fin qui descritto è mutato ra-

di Sicurezza Cibernetica (PSNC) originariamente attribuiti dal d.l. 105/2019 alla Presidenza del Consiglio dei ministri (successivamente trasferiti in capo all'ACN dal d.l. 82/2021). Posto che l'attuale disciplina preclude ai privati di conoscere le ragioni poste a fondamento della decisione della Presidenza del Consiglio, rendendo di fatto i 'soggetti inclusi' all'interno del Perimetro sprovvisti degli strumenti necessari per sindacare la loro inclusione all'interno del PNSC dinanzi a qualsiasi giudice, va segnalato che i gravosi obblighi attribuiti ai 'soggetti inclusi' sono oggi posti interamente a carico di quest'ultimi. Dunque, come si avrà modo di notare più avanti, l'attuale quadro normativo impone ai privati di sostenere dei costi ingenti a fronte di benefici che risultano a beneficio di tutta la collettività.

12 Si fa riferimento, in particolare, alla previsione contenuto all'interno del 'decreto aiuti *bis*' che ha attribuito al Presidente del Consiglio dei ministri il potere di adottare, una volta acquisito il parere del CISR e del COPASIR, "disposizioni per l'adozione di misure di *intelligence* di contrasto in ambito cibernetico" in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza.

13 Sull'argomento si rinvia, *ex multis*, al lavoro di Saltari 2007.

dicalmente con l'avvio di una seconda fase di politiche in materia di cibersicurezza tra cui si ricorda, a livello eurounitario, la direttiva NIS II, i regolamenti CER e DORA, le proposte note come 'Cyber Solidarity Act' e 'Cyber Resilience Act' e, sul versante nazionale, la l. 90/2024 (che in questo nuovo ciclo di politiche non può annoverarsi tra gli interventi più felici)[14].

Per quel che qui interessa, il nuovo quadro complessivo delineato dalla direttiva NIS2 ha causato un'evidente crisi del rapporto tra sicurezza nazionale e cibernetica. Crisi, quest'ultima, che può essere ricondotta alla scelta del legislatore europeo di tutelare il mercato interno attraverso n complesso di regole più incisive – tanto per ampiezza, quanto per profondità – rispetto a quelle utilizzate dagli Stati membri per garantire la sicurezza nazionale.

La complessità del quadro giuridico che caratterizza l'ordinamento multilivello di sicurezza cibernetica può cogliersi in modo plastico mettendo a confronto le sanzioni previste dal decreto istitutivo del Perimetro di Sicurezza Nazionale Cibernetica (PSNC)[15] con quelle proprie della Direttiva NIS2[16]. La violazione degli obblighi di segnalazione e condivisione delle informazioni contenute nella disciplina NIS2 comporta la momentanea sospensione dei certificati di cibersicurezza eventualmente rilasciati, la momentanea sospensione dei dirigenti dal loro incarico e una sanzione del 2% del fatturato globale (per un minimo di dieci milioni di euro) nel caso dei soggetti essenziali[17], o dell'1,4% nel caso soggetti importanti[18].

14 Le principali perplessità vanno ricollegate alla circostanza per cui, stante l'imminente scadenza del termine per il recepimento della direttiva NIS2, il legislatore nazionale abbia introdotto misure inedite volte ad aumentare il livello di cibersicurezza del Paese senza al contempo dare neppure un'attuazione parziale alla 'nuova' direttiva (la quale, come detto, è stata recepita successivamente con il d.lgs. 4 settembre 2024, n. 138).

15 D.l. 23 luglio 2019, n. 105, convertito con modificazioni dalla l. 16 settembre 2019, n. 126, recante "misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19 e per l'esercizio in sicurezza di attività sociali ed economiche".

16 Si rimanda, in particolare, al contenuto degli artt. 34-36 dir. (UE) 2022/2555. Vale la pena precisare che le disposizioni in esame hanno natura *self-executing* in funzione di quanto indicato dall'art. 34, par. 8, dir. (UE) 2022/2555, secondo il quale "[s]e l'ordinamento giuridico di uno Stato membro non prevede sanzioni amministrative pecuniarie, lo Stato membro in questione provvede affinché il presente articolo possa applicarsi in maniera tale che l'azione sanzionatoria sia avviata dall'autorità competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità competenti".

17 Art. 34, par. 4, dir. (UE) 2022/2555. I 'soggetti essenziali' sono stati identificati dall'art. 3, par. 1, dir. (UE) 2022/25555 come quei soggetti la cui interruzione di servizio avrebbe un impatto diretto e immediato sul funzionamento della società e dell'economia (imprese pubbliche o private operanti nel settore dell'energia, dei trasporti, della salute e della fornitura di acqua, ma anche tutte le amministrazioni centrali dei Paesi membri).

18 Art. 34, par. 5, dir. (UE) 2022/2555. I 'soggetti importanti sono stati individuati dall'art. 3, par. 2, dir. (UE) 2022/25555 come quei soggetti titolari di funzioni di rilievo all'interno dell'economia digitale e sociale (includendo servizi digitali come motori di ricerca, *cloud computing* e piattaforme *online*) meritevoli di tutela benché non critici allo stesso livello dei 'soggetti essenziali'.

Diversamente, le sanzioni individuate dal decreto Perimetro vanno da un minimo di duecento mila euro a un massimo di poco meno di due milioni, pari a circa un ventesimo delle sanzioni previste dalla direttiva NIS II[19].

Quanto fin qui messo in evidenza permette di comprendere come, allo stato dell'arte, il rapporto tra sicurezza cibernetica e nazionale non si presti a una lettura statica e uniforme. Sul versante formale, la presenza della 'riserva di Stato' in materia di sicurezza nazionale stabilita dall'art. 4, par. 2, TUE si impone quale rigida e insuperabile linea capace di regolare i confini tra la dimensione europea e la dimensione nazionale della materia. Tuttavia, osservando il quadro normativo multilivello in materia di cibersicurezza in una prospettiva sostanziale, il descritto limite non ha permesso la creazione di un vero e proprio 'nucleo duro' di funzioni di prerogativa statale volte a introdurre delle misure più stringenti (in ragione della particolare rilevanza degli interessi nazionali in gioco). Così, in nome della tutela del mercato interno dell'UE, nell'introdurre misure più dissuasive rispetto a quelle utilizzate dagli Stati membri per la tutela della sicurezza nazionale, la nuova fase di politiche di *cybersecurity* ha determinato una crisi del rapporto tra le categorie prese in esame e – come immediata ricaduta – un cortocircuito nella distribuzione di competenze a livello verticale.

4. Considerazioni conclusive sul futuro prossimo della sicurezza cibernetica

L'impossibilità di offrire una lettura univoca del rapporto tra sicurezza nazionale e sicurezza cibernetica richiede ulteriori considerazioni sul futuro prossimo della sicurezza cibernetica.

Anzitutto, l'impossibilità di individuare dei confini certi all'interno della materia rispetto alla componente assimilabile alla 'sicurezza nazionale' crea dei problemi piuttosto evidenti con riferimento al ruolo '*whole of society*' attribuito ai privati dalla Strategia Nazionale[20]. Difatti, a meno di accettare la configurabilità in astratto di un esercizio privato di funzioni pubbliche in tale materia, fissare uno spazio all'interno della *cybersecurity* riservato alla 'sicurezza nazionale' equivale a individuare un'area in cui è precluso l'intervento di attori estranei al 'comparto sicurezza'. In tal senso, i sostenitori delle capacità dello 'Stato innovatore'[21] potrebbero obiettare che lo stesso sviluppo della tecnologia internet sia stato in qualche modo frutto di un'attività di esternalizzazione della sicurezza nazionale[22], ma questa posizione può essere avallata

19 Art. 1, comma 9, lett. b), d.l. 105/2019 secondo cui "il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera a), nei termini prescritti, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000".

20 ACN, *Strategia Nazionale di Cybersicurezza*, 2022, 8, ove precisa che "la presente strategia è ispirata ad un approccio "*whole-of-society*", che vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza".

21 Il riferimento non può che essere al noto lavoro di Mazzuccato 2018 [2014].

22 Come è noto, la rete oggi conosciuta come Internet è nata all'inizio degli anni Sessanta nell'ambito di un progetto militare in cui, almeno in una prima fase, gli Stati Uniti d'America si

solo tenendo in considerazione la circostanza per cui proprio lo Stato innovatore sia finito per attribuire – seppur per un periodo ben circoscritto – a un singolo individuo il controllo esclusivo di una delle tecnologie più rivoluzionarie della storia[23]. Ciò non significa necessariamente opporsi a un maggiore coinvolgimento dei privati in questioni di sicurezza nazionale in senso ampio. Infatti, l'assenza di competenze specialistiche nel settore pubblico rende difficili gli sforzi delle amministrazioni di fronteggiare le sfide sempre più complesse poste dalla cibersicurezza.

Nonostante questa esigenza di competenze, è fondamentale definire una chiara linea di demarcazione tra pubblico e privato, capace di prevenire il ripetersi di errori del passato, come l'attribuzione incontrollata di funzioni strategiche a soggetti privati. La definizione di tali confini – è bene specificarlo – non deve però essere vista come una limitazione alla collaborazione tra pubblico e privato, bensì come uno strumento di garanzia per entrambe le parti, volto a proteggere gli interessi nazionali senza sacrificare l'innovazione o la flessibilità. La chiave sta nel costruire un quadro normativo che sia sufficientemente solido da garantire la sicurezza, ma al tempo stesso abbastanza flessibile da permettere un adattamento continuo alle innovazioni tecnologiche. Solo in questo modo sarà possibile costruire una governance della cibersicurezza capace di rispondere efficacemente alle sfide moderne, evitando sia l'eccessiva regolamentazione che la deregulation indiscriminata, e preservando così settori vitali per la sicurezza del Paese.

In secondo luogo, il contesto fin qui descritto richiede di interrogarsi circa l'opportunità di mantenere intatto il PSNC così come disegnato dal d.l. 105/2019 o se, invece, propendere verso un maggiore avvicinamento tra la dimensione nazionale e quella europea di sicurezza cibernetica. A tal proposito, se è vero che il legislatore del 'decreto Perimetro' ha elaborato tale meccanismo allo scopo di fornire un livello di tutela adeguato a quei soggetti pubblici e privati la cui attività è stata ritenuta essenziale ai fini della salvaguardia della 'sicurezza nazionale', va ricordato che il Perimetro è stato introdotto in un contesto emergenziale per porre rimedio ad alcune gravi lacune della direttiva NIS del 2016. Difatti, in una prima fase delle politiche in materia di cibersicurezza, il PSNC ha assunto un ruolo di indiscuti-

sono limitati ad essere 'promotori' dello sviluppo della tecnologia (finanziando e vigilando sul lavoro svolto da numerosi soggetti privati distribuiti in tutto lo Stato). In un secondo momento, nondimeno, le 'antiche sovranità' e i 'padri della rete' sono entrati in conflitto nel momento di stabilire quale soggetto dovesse mantenere il controllo della rete.

23 Il riferimento è agli eventi degli anni Novanta che videro protagonista uno tra i fondatori della rete, Jon Postel, ritenuto da alcuni niente di meno che "il Dio dell'Internet" [Goldsmith e Wu 2006: 29-46]. A fronte della pretesa degli Stati uniti di acquisire un maggiore controllo sulla rete, Postel decise di sfidare l'amministrazione americana con l'obiettivo di dimostrare che il ruolo dei 'fondatori' non potesse essere sostituito dagli strumenti tradizionali in possesso delle antiche sovranità. Così, attraverso una semplice email destinata a dodici operatori sparsi in tutto il mondo, un solo individuo ottenne il controllo – *rectius*, il potere di 'nominare e numerare' (la '*root authority*') – di una delle tecnologie più rivoluzionarie della storia dell'umanità. Sebbene Postel abbia 'volontariamente' rinunciato a tali poteri dopo circa una settimana, la vicenda che lo vede coinvolto merita di essere tenuta in adeguata considerazione nel dibattito sull'esternalizzazione. Per uno studio di ampio respiro sul tema dell'*internet governance* non può che rinviarsi a Carotti 2016.

bile centralità nell'infrastruttura legislativa multilivello, in quanto ha permesso di estendere alcuni obblighi di notifica degli incidenti e di certificazione anche agli 'illustri esclusi' dalla prima direttiva europea (la quale, come già ricordato, non includeva neppure le pubbliche amministrazioni).

Cionondimeno, nell'attuale quadro normativo – in cui le misure poste a tutela della sicurezza nazionale risultano meno incisive rispetto a quelle introdotte per proteggere il mercato interno dell'Unione – non risulta affatto complicato contestare la ragion d'esistere del Perimetro di sicurezza nazionale cibernetica. Difatti, nell'attesa di comprendere le modalità di attuazione a livello nazionale delle principali novità introdotte dalla direttiva NIS II, non si può fare a meno di notare come allo stato dell'arte il Perimetro produca una duplicazione degli oneri posti in capo ai soggetti 'perimetrati' (e sottoposti parallelamente al regime NIS) difficilmente giustificabile alla luce della più ampia portata delle nuove disposizioni europee. Nel contesto descritto, le entità sottoposte contestualmente alle misure nazionali ed europee sono soggetti a una gravosa duplicazione degli oneri di *compliance* e di notifica (il cui costo ricade interamente sugli stessi).

Tale circostanza dà luogo a due ordini di problemi tra loro strettamente collegati. In primo luogo, lungi dal ridurre lo sforzo richiesto ai privati per sostenere la sicurezza cibernetica italiana ed europea, il quadro normativo vigente chiede a quest'ultimi maggiori sacrifici individuali volti al raggiungimento di un'utilità diffusa (orientando il complesso di politiche italiane verso una direzione contraria rispetto alle ambizioni dell'Unione). In secondo luogo, spostando l'attenzione sui soggetti pubblici 'perimetrati', la duplicazione degli oneri aumenta ulteriormente il divario tra il grado di conoscenza richiesta alla pubblica amministrazione e la realtà del pubblico impiego italiano, il quale – oltre a non possedere una cultura informatica elementare – si dimostra oggi incapace di assorbire le competenze specialistiche richieste per far fronte alle sfide del nuovo millennio. Quest'ultima circostanza si traduce in una generale tendenza delle amministrazioni sottoposte agli obblighi PSNC e NIS a una significativa esternalizzazione degli oneri richiesti in favore di soggetti privati specializzati, il che dà luogo a un rapporto di forte dipendenza dell'apparato pubblico rispetto a un *know how* destinato a rimanere in buona parte prerogativa dei privati (strategia che nel lungo termine non può che dimostrarsi perdente)[24].

Per concludere è possibile evidenziare come, allo stato dell'arte, non sia possibile offrire una rappresentazione del rapporto tra la sicurezza cibernetica e nazionale capace di offrire una visione statica e ordinata della disciplina multilivello della cibersicurezza. Ad oggi i due concetti sono avvicinati da una forza centripeta frutto, sul piano nazionale, del progressivo allontanamento della materia dal Sistema di Informazione per la Sicurezza della Repubblica (SISR)[25] e, sul versante euro-unita-

24 Per un'analisi volta a rappresentare le sfide della collaborazione pubblico-privato nel settore della cibersicurezza si rimanda, tra gli altri, a Previti 2022: 65-93.

25 Il Sistema di Informazione per la Sicurezza della Repubblica (SISR) è l'infrastruttura disegnata dalla legge l. 3 agosto 2007, n. 124 allo scopo di riorganizzare l'assetto del 'comparto *intelligence*' italiano che, fino a quel momento, aveva operato sotto la vigenza l. 24 ottobre 1977, n. 801.

rio, dal contestuale indebolimento (superamento?) del dogma della 'prerogativa di Stato' in materia di sicurezza nazionale di cui all'art. 4, par. 2, TUE[26].

Le peculiarità che caratterizzano lo stato dell'arte della disciplina in commento non devono tuttavia disincentivare ulteriori studi volti ad approfondire la relazione in oggetto. Non solo, come messo in evidenza *supra*, le modalità con cui tale rapporto viene declinato hanno delle conseguenze profonde a livello pratico ricollegate soprattutto alla distribuzione di competenze verticali (tra Unione europea e Stati membri) e orizzontali (tra pubblico e privato) e assumono grande rilievo anche sul versante teorico generale. Del resto, se è vero che le istituzioni nazionali ed europee si occupano di definire soltanto la nozione di 'sicurezza cibernetica', è evidente che la codificazione di questa nuova 'dimensione' della sicurezza rappresenta uno dei principali stimoli – insieme alla disciplina dei *golden powers*[27] – della nuova fase di giuridicizzazione della *national security*.

Bibliografia

Barberis M. 2017, *Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo*, Bologna: Il Mulino.

Bobbio N. 1976, "Eguaglianza ed egualitarismo", *Rivista internazionale di filosofia*, Vol. 53 (n. 3): 321-330.

Buoso E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli.

Carotti B. 2016, "Il sistema di Governo di Internet", Giuffrè: Milano.

Carotti B. 2020, "Sicurezza cibernetica e Stato-nazione", *Giornale diritto amministrativo*, (5): 629-641.

De Nitto S. 2022, "Il golden power nei settori rilevanti della difesa e della sicurezza nazionale: alla ricerca di un delicato equilibrio", *Diritto amministrativo*, (2): 553-587.

Fuster G.G., Jasmontaite GG. 2020, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights", in M. Christen, B. Gordijn and M. Loi (eds.), *The Etics of Cybersecurity*, Cham: Springer.

Giupponi T.F. 2008, *Le dimensioni costituzionali della sicurezza*, Bologna: Libreria Bonomo.

Giupponi T.F. 2024, "Il governo nazionale della cybersicurezza", *Quaderni costituzionali*, n. 2: 277-303.

Goldsmith J. and Wu T. 2006, *Tho controls the internet? Illusion of a Borderless World*, Oxford: Oxford University Press.

Longo E. 2024, "Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere", *Rassegna Parlamentare*, n. 2: 313-347.

Matassa M. 2023, "La regolazione della cybersecurity in Italia", in R. Ursi (ed.), *La sicurezza nel cyberspazio*, Milano: Franco Angeli: 21-42.

26 Cfr. Zalnieriute 2022: 198-218.

27 In estrema sintesi *golden powers* possono essere inquadrati come quei poteri speciali previsti dal d.l. 15 marzo 2012, n. 21 volti ad attribuire al Governo italiano il potere di dettare specifiche condizioni all'acquisto di partecipazioni, di porre veto all'adozione di determinate delibere societarie e di opporsi all'acquisto di partecipazioni (oggi disciplinati al livello europeo dal regolamento 2019/452). Per un approfondimento sull'esercizio dei poteri speciali nei settori della difesa e della sicurezza nazionale si rimanda a De Nitto 2022: 553-587 e Matassa 2024: 325-352.

Matassa M. 2024, "I golden powers italiani nel settore della difesa e sicurezza nazionale", *Il diritto dell'economia*, Vol. 113 (1): 325-352.
Mazzuccato M. 2018 [2014], *Lo Stato innovatore*, Roma-Bari: Laterza.
Monti A. 2020, "Internet e ordine pubblico", in G. Cassano, S. Previti (eds.), *Il diritto di internet nell'era digitale*, Milano: Giuffré Francis Lefebvre: 51-80.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", *federalismi.it*, (25): 65-93.
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica.
Saltari L. 2007, *Amministrazioni nazionali in funzioni comunitarie*, Milano: Giuffrè.
Serini F. 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto legge n. 82 del 2021", *federalismi.it*, (12): 241-272.
Ursi R. 2022, *La sicurezza pubblica*, Bologna.
Ursi R. 2023, "La sicurezza cibernetica come funzione pubblica", in R. Ursi (ed.), *La sicurezza nel cyberspazio*, Milano: Franco Angeli: 7-20.
Zalnieriute M. 2022, "A struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union", *Modern Law Review*, Vol. 85 (n. 1): 198-218.

Andrea Mattarella

Il Cybercrime tra nuovi paradigmi e tutela della vittima vulnerabile. Opportunità e limiti della Restorative Justice

Abstract: La rivoluzione digitale ha generato un universo alternativo a quello fisico, privo dei riferimenti spaziali e temporali di cui il diritto penale si nutre. Rispetto alle categorie tradizionali, i cybercrimes presentano alcuni caratteri di specialità. Notevoli implicazioni sistematiche discendono dalla permanenza del dato digitale nel cyberspazio, che comporta un peculiare atteggiarsi dell'offesa penalmente rilevante; ciò comporta uno spostamento dell'analisi dall'autore del reato, che grazie alle TIC può essere anche un soggetto privo di particolari caratteristiche criminali, alle vittime vulnerabili. Per i delitti contro la persona, un approccio attento a tutti i soggetti coinvolti e alla reale offensività delle condotte impone di pensare anche ad altri strumenti per gestire il conflitto derivante dal reato. Pur non potendo garantire risultati efficaci per ogni forma di reato, la mediazione presenta delle potenzialità notevoli in termini di ascolto delle vittime, auto-responsabilizzazione del reo e special-prevenzione rispetto ad alcuni fenomeni criminali connessi alla rete.

Keywords: Cybercrime; Cyberspazio; Danno; Restorative Justice; Mediazione.

1. Le peculiarità dei reati commessi nel cyberspazio. la permanenza in rete del dato digitale e l'offesa alla persona

Mutuando la definizione di società moderna come società liquida del sociologo Baumann, il *cybercrime* costituisce il paradigma della dimensione liquida e senza confini della criminalità moderna[1]. Con la globalizzazione, ha infatti preso vita un universo alternativo a quello fisico, privo dei riferimenti spaziali e temporali di cui il diritto penale si nutre, che alcuni studiosi definiscono come un "non luogo" privo di rigide regolamentazioni[2]; tuttavia, proprio per la rapidità di comunicazione e l'anonimato che assicura, la rete dimostra innate potenzialità criminogene. I rischi principali derivano non solo dalle organizzazioni criminali, ma anche dagli utenti occasionali del *web*.

1 Baumann 1990.
2 Ingrassia 2012: 2

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760162

La criminalità informatica, pur essendo citata nelle normative nazionali e internazionali, non consiste in una categoria giuridica compiutamente definita. Una ricostruzione dottrinale distingue tra i reati informatici in senso stretto ed i reati informatici in senso ampio[3]. Nei primi, tipizzati attorno a procedimenti di automatizzazione di dati o informazioni, ovvero a modalità o oggetti tecnologici, l'uso delle tecnologie informatiche costituisce elemento costitutivo. I secondi configurano reati realizzabili anche *"offline"*, ma che acquistano maggiore lesività se commessi con l'utilizzo dei predetti mezzi. Una parte della dottrina americana suddivide i *cybercrimes* in tre categorie, a seconda che il sistema informatico costituisca l'obiettivo della condotta illecita ovvero lo strumento per preparare un reato, o sia solo un aspetto incidentale nella commissione dell'illecito[4].

In questa sede si intendono evidenziare i profili di specialità dei reati informatici, per comprendere quali strumenti siano utilizzabili da un diritto penale saldamente inscritto nel solco dei principi costituzionali di fronte alle insidie dovute alle nuove tecnologie, la cui impressionante evoluzione decreta l'obsolescenza delle normative ed erode la tenuta degli istituti tradizionali.

La legislazione italiana in materia di *cybercrime* si basa sostanzialmente sulla legge 547 del 1993, che ha operato un'integrazione delle norme del Codice penale, in assenza di un disegno più organico che tenesse conto delle specificità delle fattispecie in esame[5].

Uno dei pilastri messi in crisi dal cyberspazio è la funzione di orientamento in cui si sostanzia la finalità di prevenzione generale del diritto penale. Grazie alle possibilità di informazione e comunicazione offerte dalla rete, alcuni delitti come la diffusione di materiale pedopornografico o la diffamazione si trasformano in fenomeni di massa, commessi in modo seriale, i cui autori appartengono ad ogni classe sociale e non percepiscono il disvalore delle proprie condotte; a ciò consegue una ridotta disapprovazione da parte dei consociati e una cifra nera altissima, per la difficoltà di individuare gli autori[6].

3 Picotti 2000; Pecorella 2006; Picotti 2018: 75 ss.; Picotti 2004: 21 ss.; Flor 2019: 75; Sieber 2012: 18 ss.

4 Un inquadramento generale si deve a Clough 2015: 11ss.; Weismann 2011; Brenner 2006: 17.

5 Per i reati *cyber* correlati, l'adeguamento della tecnica legislativa all'evoluzione tecnologica appare più semplice, consistendo generalmente nell'utilizzo di circostanze aggravanti per l'utilizzo di mezzi informatici: può farsi l'esempio dello *stalking*, concretizzabile in una persecuzione della vittima attraverso *computer*, *smartphone* o *social network*, o di tutte le forme di truffa o estorsione, in cui gli artifizi, i raggiri, e le minacce vengono veicolate attraverso messaggi in rete. I reati cyberdipendenti possono offendere il patrimonio, la persona, i diritti di proprietà intellettuale o persino integrare il cyberterrorismo e il *cyber warfare*. Per i delitti contro la persona, occorre citare la produzione, il possesso e la diffusione di materiale pedo-pornografico, regolato dagli articoli 600-*ter* c.p. e 600-*quater* c.p, l'adescamento di minori attraverso la rete, previsto dall'art. 609-*undecies* c.p. e il *revenge porn*, di cui al nuovo art. 612 *ter*. Queste fattispecie pongono il problema di identificare i responsabili e di bloccare la diffusione dei contenuti sensibili e le condotte aggressive, per l'impatto devastante dei mezzi telematici sulla sfera personale.

6 Sul concetto di reati di massa si veda Paliero 1985:181 ss., che richiama a sua volta Hellmer 1972: 21 ss.; il concetto di "cifra nera" è rilevato da Spagnoletti 2004: 1922 ss.

Un secondo pilastro a cedere è quello del *locus commissi delicti*. La rete configura un ambiente immateriale non delimitato entro ambiti fisici o territoriali, accessibile da una molteplicità di postazioni remote. Ne consegue che un reato informatico può essere potenzialmente pianificato in qualsiasi Stato, essere realizzato in un altro paese e produrre i propri effetti in un terzo Stato. Rispetto alle condotte attive tradizionalmente intese, caratterizzate da un substrato materiale e da un'incorporazione dell'accadimento materiale, le condotte tenute nel cyberspazio si caratterizzano per una "dematerializzazione", "velocizzazione", "deterritorializzazione", "detemporizzazione" e "ubiquità"[7]. La dimensione *cross-border* dei reati informatici limita la capacità di reazione dello Stato; secondo alcuni autori, tale problematica può essere risolta attraverso un'interpretazione evolutiva del principio di territorialità per adattarlo allo spazio digitalizzato o un intervento legislativo che eviti interpretazioni estensive delle norme sulla competenza e sulla giurisdizione[8].

Di conseguenza, una terza peculiarità della rivoluzione informatica per il diritto penale è l'inasprirsi della crisi dei sistemi fondati sullo Stato-Nazione. Da tempo la dottrina riscontra una trasformazione della relazione tra territorio e sovranità e tra territorio e legge[9]. Con una criminalità senza confini, la sovranità degli Stati nel regolare le condotte umane è entrata ulteriormente in crisi, portando all'estremo l'esigenza di un nuovo assetto di governo delle dinamiche sociali ed economiche e di una internazionalizzazione del contrasto ai reati.

In stretta connessione con l'ultimo tema, la rivoluzione digitale ha implementato il ruolo dei soggetti privati nella *governance* dei rischi dello spazio cibernetico. L'universo digitale, inondato da una mole spropositata di dati e informazioni riversate nel *web*, ha assottigliato il confine tra pubblico e privato. La globalizzazione, indebolendo la capacità normativa e regolatoria degli Stati, ne ha determinato il ritiro dalla gestione di interi settori economici con il conferimento a soggetti privati, dalle dimensioni e capacità finanziarie sempre più imponenti, di funzioni di prevenzione dei reati e di *risk management*[10]. Questo processo di istituzionalizzazione dell'ente è esaltato dall'affermazione del cyberspazio come luogo di scambio di beni e servizi e di diffusione delle informazioni, del quale i principali protagonisti per risorse e competenze sono le imprese multinazionali. Ne consegue, in primo luogo, l'espansione dell'area della responsabilità degli enti e del modello della *com-*

7 Picotti, 2011, 217 ss. Per quanto concerne le condotte omissive, invece, occorre evidenziare che secondo la prevalente dottrina assumono essenza non naturalistica, ma normativa, consistendo nel mancato compimento di un'azione che si ha l'obbligo giuridico di compiere, ossia nel giudizio normativo di difformità del comportamento tenuto rispetto al comando legale. Sul punto, cfr., *ex multis*, Marinucci, Dolcini, Gatta 2019: 257 ss.; Fiandaca, Musco 2024: 636-637; Marinucci 2009: 523 ss.

8 Flor 2019:192.

9 Tra i tanti contributi, cfr. in particolare, Schmitt 1995: 108 ss.; Kumar Sen 2009; Di Martino 2010: 74 ss.

10 Nella letteratura straniera, in particolare, Power 2004: 13 ss.; Miller 2017: 446; Caldwell 2020; nella dottrina italiana, senza pretesa di esaustività, Colacurci 2022: 75; Giorgino, Pozza 2017: 103 ss.; Corbella, Pozza 2016: 52 ss.

pliance. La dottrina[11] ha utilizzato l'espressione di delega di autoregolamentazione, per indicare che l'ente partecipa dei compiti di prevenzione, gestione e contenimento del rischio alla base dell'organizzazione aziendale, propri delle autorità statali. Sebbene una parte consistente degli attacchi cibernetici abbia le imprese come bersaglio, va rilevato come spesso l'ente possa essere beneficiario della realizzazione di un reato informatico posto in essere da un suo apicale o sottoposto.

In secondo luogo, la difficoltà di impedire la diffusione in rete di contenuti illeciti e di individuare i responsabili rende indefettibili meccanismi di collaborazione e modelli di responsabilità penale degli *internet providers*. Sono stati teorizzati due modelli astratti di responsabilità, rispettivamente a titolo commissivo e omissivo[12]. Il primo ricorre nell'ipotesi in cui si dimostri che l'*internet provider* abbia agevolato l'immissione in rete del materiale, d'intesa con chi materialmente lo abbia inserito a mezzo di sistema informatico e telematico[13]. Questa impostazione si presenta maggiormente garantista, ma incontra la difficoltà di provare l'accordo tra il gestore della rete ed il soggetto che vi ha inserito i contenuti penalmente rilevanti[14]. Il secondo modello concerne una responsabilità penale per omissione dell'*internet provider*, che si basa sulla prova che quest'ultimo ha omesso un controllo sul materiale inserito in rete, secondo lo schema dell'omesso impedimento dell'evento di cui all'art. 40, comma 2, c.p. La dottrina considera questa soluzione più agevole sul piano probatorio, ma evidenzia sul piano soggettivo la problematicità per l'*internet provider* di conoscere il carattere illecito di un contenuto prima che siano immessi definitivamente in rete[15].

Ciò premesso, il profilo che, ad avviso di chi scrive, è meritevole di particolare approfondimento, per le sue implicazioni sistematiche, discende proprio dalla – tendenzialmente – definitiva permanenza del dato digitale nel cyberspazio, che comporta, sotto il profilo strutturale, un peculiare atteggiarsi dell'offesa penalmente rilevante; quest'ultimo aspetto comporta uno spostamento dell'analisi dall'autore del reato, che grazie alle TIC può essere anche un soggetto privo di particolari vocazioni criminali, alle vittime vulnerabili, con delle precise ripercussioni in ordine ai rimedi che il diritto penale può adottare.

L'automazione che caratterizza l'elaborazione, la circolazione, la messa a disposizione e la permanenza dei dati in rete condizionano la consumazione stessa del reato. Da un lato, si espandono gli effetti del reato nel tempo e nello spazio; dall'altro lato, si osserva come lo stesso fatto tipico, realizzandosi grazie agli strumenti informatici, si protrae e si riproduce, senza una completa dominabilità dei gestori e dei fruitori dei sistemi. Questa forma di "permanenza" del reato cibernetico e di espansione degli effetti non configurerebbe un mero *post factum* non punibile, perché il prolungamento della condotta e dell'evento tipico dovuto all'automazio-

11 Gobert, Punch 2003: 315 ss.; Ayres, Braithwaite 1992: 101 ss.; Bamberger 2006: 386; Fiorella 2012: 14 ss.; Fiorella, Selvaggi 2018: 12; Gullo 2021: 245.

12 V., *ex multis*, Manna 2010: 779 ss.; Seminara 2014; Manna, Florio 2019: 901 ss.

13 Piergallini 2015: 779.

14 Manna: 2010, 780; Manna, Florio 2019: 902.

15 Manna, *ibidem*; Manna, Florio, *ibidem*.

ne non acquisisce autonomia rispetto alle altre componenti del reato. Parte della dottrina propende per un adattamento alla realtà cibernetica della tradizionale distinzione tra momento di perfezione formale del reato, quando ne sono realizzati tutti gli elementi costitutivi, e la fase di consumazione, quando si esaurisce definitivamente l'offesa specifica, per avere il reato raggiunto il massimo grado di lesione del bene giuridico protetto[16]. In tal senso, il reato informatico non può considerarsi esaurito nel periodo intermedio, che può essere molto lungo, intercorrente tra i due momenti, in cui l'offesa permane e si approfondisce.

Questo fenomeno non è inquadrabile *in toto* nel paradigma del reato permanente, il quale presupporrebbe la costante dipendenza della protrazione dell'offesa al bene giuridico dalla condotta volontaria del reo, in grado in ogni momento di farla cessare[17]. Diversamente dal modello in esame, per effetto della diffusione automatica dei contenuti nella rete, gli effetti della condotta inizialmente posta in essere dal reo sfuggono al suo controllo.

La tesi proposta non ritiene utilizzabile nemmeno la categoria del reato a consumazione prolungata, affermatasi in giurisprudenza in relazione a fattispecie caratterizzate da un doppio schema alternativo di consumazione, come la corruzione e l'usura, ove la promessa può essere seguita da pagamenti, i quali devono considerarsi parte del momento consumativo; in tali ipotesi, gli atti successivi all'accordo o alla promessa sono comunque ricollegabili alla volontà del reo, laddove la diffusione incontrollata dei dati nel cyberspazio sembra sfuggire al dominio volontaristico dell'autore[18].

A questa prospettazione potrebbe replicarsi facendo riferimento alle ipotesi in cui l'agente, versando in dolo eventuale o diretto, immetta dei contenuti in rete accettando che essi raggiungano potenzialmente ogni dispositivo connesso. Tuttavia, la dottrina in commento evidenzia la necessità di delineare un differente paradigma, che spieghi la peculiare realtà della diffusione e comunicazione di pensieri e informazioni in rete, nella quale non rileva un evento consumativo autonomamente verificabile nel mondo materiale[19]. La consumazione prolungata del reato, oltre il momento della perfezione formale, non consente di ravvisare gli elementi della condotta tipica, che dovrebbe ricondursi ad un dominio volontaristico attuale. Tuttavia, si rileva che l'offesa è pur sempre conseguenza diretta di una condotta volontaria realizzata nel cyberspazio; si individua, pertanto, una peculiare accezione di evento che, pur consumandosi nella rete, conserva tutte le caratteristiche di rilevanza nello spazio fisico, in termini di offesa agli interessi protetti e di effetti sulla vittima.

La severità dell'impatto sulla vittima della condotta aggressiva posta in essere grazie alla facilità e rapidità di comunicazione della rete soprattutto nei casi in cui questa consista nella divulgazione di dati personali o immagini intime, legittima,

16 Picotti 2019: 91, che cita Carrara, 1874: 229 ss., nonché Jescheck, Weigend 1996: 517 ss.

17 Sulle conseguenze della durata nel tempo delle caratteristiche del reato permanente ed altri reati di durata, cfr. Romano 2004: § 118s., 344 s.

18 Picotti 2019: 92; per un quadro della questione, v. Brunelli 2000.

19 Picotti, *ibidem*.

sul terreno dell'offensività e della sussidiarietà, l'intervento penale. La cifra distintiva di reati come la diffamazione *online*, la pedopornografia virtuale, le forme di diffusione non consensuale di immagini intime, nonché delle molteplici violazioni della riservatezza e della *privacy* risiede nell'irrimediabilità della pubblicazione: una volta *online*, le immagini non conoscono oblio[20]. Questa degenerazione delle nuove tecnologie espone la persona a nuove forme di rischio[21]. Utilizzando come modello di riferimento l'ampio genere della pornografia non consensuale, a dispetto di una preponderanza di indagini con un approccio criminologico incentrato sull'autore[22], alcuni studi mostrano come l'80% delle vittime soffrirebbe di *stress* emozionale ed ansia[23], mentre il 47% penserebbe almeno una volta al suicidio[24]. Alla pubblicazione si accompagna spesso il c.d. *doxxing*, ovvero la tendenza dei fruitori dei materiali a pubblicare non solo le immagini intime, ma anche informazioni personali della persona raffigurata, che diventa bersaglio anche di *stalking* e *hate crimes*[25]. A causa del danno reputazionale, un'altra conseguenza frequente è la perdita del lavoro o il ritiro delle vittime dagli spazi pubblici. Per illustrare la tendenziale irrimediabilità dell'offesa arrecata alla persona, la dottrina statunitense ha affermato che la permanenza in rete dei materiali pornografici trasforma "*an original sin into an eternal one*"[26].

La vulnerabilità delle vittime chiarisce non solo il ruolo di deterrenza che può essere svolto dal diritto penale, ma anche l'insufficienza di un approccio esclusivamente retributivo, incentrato sull'autore da assoggettare a pene sproporzionate, che ha segnato talvolta la legislazione italiana.

Sotto tale profilo, il tema della criminalità informatica riporta alla luce un dibattito dalle radici antiche, rappresentato dalla necessità di un mutamento di prospettiva rispetto al tradizionale disinteresse del diritto penale per la vittima. Con la pubblicizzazione del diritto e del processo penale, il ruolo di tale soggetto viene marginalizzato, divenendo protagonisti il reo e lo Stato titolare del monopolio della sanzione[27]. Questa riscoperta della vittima è un'occasione per riaffermare scelte incriminatrici ancorate ai principi costituzionali e per potenziare l'orizzonte della giustizia riparativa: se lo scopo del diritto penale è tutelare i beni giuridici preve-

20 Cfr. Larkin 2014: 62 ss., citato da Caletti 2018: 81.

21 V. Citron, Franks 2014: 347;

22 Lo rileva Gillespie 2016: 220. Uno studio condotto da medici psichiatri è quello di Kamal, Newman 2016: per l'analisi dei risvolti medici, soprattutto, 362 ss.

23 Si vedano le statistiche proposte da Citron e Franks 2014: 351.

24 Barmore 2015: 449.

25 In proposito, McGlynn, Rackley 2017: 545. Il termine "*doxxing*" indica la pratica di diffondere *online* informazioni personali o altri dati sensibili, in contesti talvolta di "*online shaming*".

26 Cfr. Larkin, *ibidem*. Sull'irrimediabilità del danno, per alcune forme di incriminazione in ambito pedopornografico. Cfr. Picotti 2007: 1292, evidenzia come, nel "nuovo contesto di rapporti sociali permeati dalla tecnologia delle comunicazioni a distanza, "globalizzate" e capillari, disponibili a chiunque, emerge la necessità di vietare ab origine la produzione del materiale illecito in quanto "pedo-pornografico", a prescindere dalla genesi della sua creazione nello sfruttamento od anche mera utilizzazione della vittima".

27 Venturoli 2015: 8; Venafro 2004: 12.

nendone l'offesa, la comprensione dei fenomeni illeciti connessi alla rete sarebbe incompleta senza lo studio della vittima[28].

Già nelle fonti internazionali ha cominciato a farsi strada un concetto di vittima più ampio della nozione di soggetto passivo del reato; questa non deve solo essere tutelata, ma anche partecipare attivamente al procedimento penale, intervenire nella richiesta di restituzione e riparazione dei danni ed essere attrice nella risoluzione dei conflitti verificati in seguito ad un reato. Un esempio delle istanze di tutela della persona emergenti dai reati informatici è offerto dalla Convenzione contro il *cybercrime* in corso di approvazione presso l'ONU che prevede obblighi di incriminazione e di cooperazione tra i paesi e forme di assistenza alle vittime di reato[29].

Anche nella legislazione italiana recente, e in particolare rispetto ai fenomeni criminali connessi alla rete, emerge una maggiore attenzione verso la vittima del reato. Tuttavia, più che ad un'attenta considerazione degli effettivi bisogni di tutela delle persone attinte dal reato, la legislazione italiana di dichiarata ispirazione vittimologica, specie rispetto a reati commessi in rete, si è caratterizzata per una carica fortemente simbolica e per una caratterizzazione soggettiva degli illeciti penali, in contrasto con i principi di proporzionalità ed offensività. Dal punto di vista sostanziale, le norme *victim oriented* si sono caratterizzate non di rado per l'incriminazione della mera violazione di precetti piuttosto che della lesione di beni giuridici e per un'intensa carica simbolica, in quanto dirette a formulare una pronta risposta legislativa a istanze di incriminazione provenienti dalle vittime.

È emblematico di queste fattispecie focalizzate sul disvalore di azione il delitto di pedopornografia virtuale di cui all'art. 600-*quater*.1 c.p., che punisce anche la mera detenzione per uso personale di immagini pedopornografiche raffiguranti non già soggetti reali di minore età, ma mere rappresentazioni di elaborazione grafica. Come si è osservato, la predetta disposizione difetta di una tangibile offesa alla persona reale del minore, e si risolve sostanzialmente nella punizione di un tipo di autore, il pedofilo virtuale, che manifesta una particolare immoralità e riprove-

28 Venturoli 2021: 26. Lamanuzzi 2015, rileva che lo studio della vittima è funzionale alla comprensione della dinamica del fatto e all'accertamento delle responsabilità e consente di individuare le specifiche esigenze di protezione *post-delictum* di chi abbia subito un reato, nonché la riduzione dei rischi di vittimizzazione secondaria e di multi-vittimizzazione. Lo studio delle vittime influisce anche sulla riforma delle norme esistenti e di introduzione di nuove fattispecie incriminatrici. V. anche Parziale 2020: 10.

29 L'inventario delle incriminazioni spazia dalle "classiche" fattispecie di c.d. "*cyber-dependent crimes*",ai c.d. "*cyber-enabled crimes*". Le disposizioni a tutela dei minori dagli abusi sessuali in rete, concentrata negli articoli 14, 15 e 16, relative ad abuso e sfruttamento sessuale di minori attraverso il sistema informatico, adescamento di minori e diffusione non consensuale di immagini intime, offrono utili indicazioni sulla protezione da offrire alle vittime vulnerabili. L'articolo 34 prevede le misure di assistenza e protezione delle vittime, in particolare nei casi di minaccia di ritorsioni o intimidazioni, per garantire l'accesso al risarcimento, il coinvolgimento delle vittime nelle fasi del processo penale. Con riferimento ai delitti di pornografia minorile, si fa riferimento alla necessità di tenere in considerazione le esigenze dei minori, con forme di assistenza fisica e psicologica e di rimozione o di inaccessibilità dei contenuti pedopornografici.

volezza[30]. Una parte della dottrina cita in questo senso il d. l. 93/2013 in materia di femminicidio e, nell'ambito dei *cybercrimes*, le manifestazioni di discriminazione o di *hate speech* realizzate nel *web*[31]. Sul piano sanzionatorio, questo tipo di legislazione si caratterizza per pene sbilanciate verso la finalità di prevenzione generale e distaccate dalla funzione di protezione di beni giuridici e di risocializzazione[32], che comportano una torsione del modello del diritto penale liberale: modellare il fatto e la sua capacità offensiva sulla percezione della singola vittima equivale infatti a fuoriuscire dal perimetro della tipicità[33]. Un tale operare non elimina alla radice i fattori criminogeni alla base di talune manifestazioni illecite.

Consultando i dati offerti nel 2023 dal *Centro Nazionale per il Contrasto alla Pedopornografia online* (*C.N.C.P.O.*) della Polizia Postale e delle Comunicazioni, possono cogliersi alcune linee di tendenza della criminalità informatica in generale, e in particolare dei reati in danno di una categoria particolarmente esposta come i minori. Le denunce relative ai casi di adescamento online, infatti, raccontano di un numero di casi in lieve flessione, ma più alto per le fasce di potenziali vittime che non superano i 13 anni. Peraltro, nel 2023 si è registrato un incremento dei casi di *sextortion*, che a differenza del passato coinvolgono sempre più frequentemente gli adolescenti, in particolare ragazzi tra i 15 e i 17 anni. Sono stati analizzati 28.265 spazi *web*, di cui 2.739 inseriti in *black list* e oscurati per la presenza di materiali pedopornografici, con un aumento rispetto ai 2662 siti oscurati nel 2022[34].

Altrettanto rilevante è il dato sul deferimento di 1224 soggetti per pedopornografia e adescamento di minori *online*. L'analisi dei dati ha rivelato una diminuzione dei casi di cyberbullismo ricollegabile anche all'opera di sensibilizzazione svolta dalle istituzioni e organizzazioni del terzo settore, nonché dalle strutture scolastiche[35]. Il *Report* evidenzia tuttavia un significativo aumento dei reati contro la persona commessi attraverso la rete, tra i quali *stalking*, diffamazione *online*, minacce, *revenge porn*, molestie, *sextortion*, illecito trattamento di dati personali, *hate speech* e istigazione al suicidio; nel dettaglio, sono poi stati segnalati 31 casi di Codice Rosso[36].

Il quadro generale descritto e la tendenziale irrimediabilità dei pregiudizi inferti al singolo individuo per effetto delle nuove tecnologie evidenziano come, per il superamento di tali forme di offesa, non è sufficiente l'irrogazione di pene severissime, in quanto questa impostazione rischia di "non dare nulla di concreto"

30 Così Brunelli 2019: 46. In argomento v. anche Cocco 2006: 863 ss.

31 Venturoli 2021: 13 e 21.

32 In questo senso, Venturoli 2021: 29; in rapporto alla correlazione tra la severità delle sanzioni minacciate e l'andamento dei tassi di criminalità, vd. Pagliaro 1985: 353 ss.; Cocco 2018: 14 ss.; sul rapporto tra pena e bene giuridico, v. Cfr. Paliero 1992: 856; Cornacchia 2010: 220 ss.; Fiandaca 1982: 42 ss.

33 Insolera 2023: 41.

34 I dati sono rilevati, rispettivamente, al 21/12/2022 e al 21/12/2023 e sono consultabili all'indirizzo https://www.interno.gov.it

35 Nel 2023 sono stati trattati 284 casi di cyberbullismo. Di contro, è stata registrata una flessione del numero dei minori segnalati all'Autorità Giudiziaria, 104 rispetto ai 127 del 2022.

36 In particolare, nel 2023 vi è stato un incremento percentuale del 3% dei casi trattati, per un totale di 9433, e del 7% delle persone indagate, che raggiungono complessivamente i 1235 casi.

alla persona offesa ma soltanto di "togliere qualcosa all'autore" attraverso processi punitivi collocati al di fuori dei principi costituzionali[37]. Ciò in quanto la pena è tradizionalmente idonea a soddisfare la vittima in via indiretta, rassicurandola con la minaccia di sanzioni severe e dissuasive nei confronti di eventuali autori di reati o appagandola con l'inflizione in concreto di una pena al reo[38]. Se per le fattispecie integranti delitti contro la personalità dello Stato, contro l'ordine o l'incolumità pubblica, attacchi contro le infrastrutture strategiche o addirittura scenari di cyberterrorismo o *cyberwarfare* risulta difficile concepire percorsi alternativi alla pena in senso stretto, per i reati informatici contro la persona un approccio attento a tutti i soggetti attinti dal reato nonché al reale grado di offensività delle condotte impone di pensare anche ad altri strumenti finalizzati ad una diretta gestione del conflitto derivante dal reato. Nell'ambito di una pena concepita in senso dinamico-prescrittivo, in vista dell'autoresponsabilizzazione e della reintegrazione sociale dell'autore, potrebbe riconoscersi un ruolo centrale alla componente riparatoria del nocumento patito dalla vittima, non limitata al danno civile[39].

2. Un possibile ruolo per il modello del delitto riparato

Il sorgere della giustizia riparativa è dovuto, in primo luogo, all'insoddisfazione per i sistemi fondati su programmi di deterrenza e sulla sanzione come unica risposta al reato, manifestata già dagli anni Sessanta da diversi giuristi americani[40]. In secondo luogo, si è rilevato che la giustizia punitiva tradizionale, incentrandosi sull'autore del reato, non consente di dare voce alle vittime delle azioni delittuose, ponendosi sempre di più l'esigenza di attribuire a queste ultime un ruolo più protagonistico nella gestione del conflitto generato dall'illecito[41]. Sotto questa angolazione, la *restorative justice* si presenta più attenta alle concrete ricadute esistenziali e ai danni arrecati alla vittima dall'illecito, che si cerca di neutralizzare con il contegno riparatore del colpevole[42].

Conseguentemente, il reato è considerato non più come un'offesa solamente allo Stato, ma anche come un'offesa alla persona, che impone la ricerca di un accordo di riparazione[43]. Tuttavia, per evitare che ciò si traduca in una deviazione dalla qualificazione formale dei fatti penalmente rilevanti, la maggior parte degli ordina-

37 Mettono in luce l'esigenza di porre un argine ad irrazionali processi di penalizzazione di ispirazione vittimocentrica Padovani 2019: 51 e Cornacchia 2012: 12.

38 Venturoli 2021: 33.

39 Cfr. Eusebi 2001: 121, per il quale la risocializzazione esige che l'intervento punitivo implichi il minor sacrificio possibile dei diritti essenziali all'inserimento sociale di ciascun individuo e, dall'altro, assuma preferibilmente modalità significative sotto il profilo dei valori di solidarietà sociale; Venturoli 2021: 32.

40 Gibbs 1963; Gulliver 1969; Lubman 1967;

41 Mannozzi 2003; Fiandaca, Visconti 2009; Mannozzi, Lodigiani 2015; Bertagna, Ceretti, Mazzucato 2015; Di Tommaso 2023; Insolera 2023.

42 Di Tommaso 2023: 26

43 Di Tommaso, *ibidem*.

menti disciplina puntualmente le condizioni di accesso alla giustizia riparativa, in una posizione accessoria rispetto alla giustizia punitiva[44]. Il modello retributivo e quello riparativo divergono anche nei criteri di valutazione degli esiti, guardando l'uno alla severità della punizione per il reato commesso, e auspicando l'altro una riconciliazione delle parti. Infine, una ragione dell'affermazione della *restorative justice* risiede anche nella crisi dei sistemi di regolazione sociale dei conflitti, dovuta alla globalizzazione ed all'economia moderna, che ha scaricato la gestione di queste problematiche sul sistema giudiziario[45]. Questo vuoto istituzionale avvertito dalla società può essere colmato attraverso la creazione di sedi ristrette dove elaborare soluzioni condivise.

Esistono molteplici tipologie di programmi a carattere riparatorio, a partire dalla presentazione di scuse formali, alle forme di incontro tra la vittima e il reo, alla mediazione allargata ai familiari della persona offesa, a piccoli gruppi di cittadini o alla comunità tutta, passando per la prestazione di attività lavorativa a favore della comunità o la corresponsione di risarcimenti e restituzioni alle vittime.

A queste figure si aggiungono gli istituti di *diversion*, caratterizzati da non secondarie finalità di deflazione processuale, oltre che dall'esigenza di sottrarre l'autore del reato agli effetti deleteri del circuito penale[46]. Gli studi italiani e angloamericani dedicano particolare attenzione, per la loro efficacia, alla *Neighbourhood justice*, al *Family Group Conferencing*, ai *Sentencing Circles*, ai *Victim Impact Statements* ed ai *Victim Offender Reconciliation Programs*, i quali mirano principalmente alla prevenzione dei reati grazie allo sviluppo delle iniziative e delle forze sociali.

Concentrando l'analisi sui *Sentencing Circles* e sui *Victim Impact Statements*, essi consentono alla vittima una maggiore visibilità nel processo, potendo esprimere il proprio punto di vista nella fase di quantificazione della pena, che negli ordinamenti di *common law* è oggetto di un'apposita udienza.

I *Victim Offender Reconciliation Programs* si caratterizzano, invece, per un più forte carattere mediatorio. Il predetto modello è nato negli Stati Uniti negli anni Settanta e si basa su un incontro tra vittima e autore del reato, finalizzato al reciproco riconoscimento ed alla riparazione, lasciando nondimeno alla volontà delle parti il raggiungimento di un accordo. Anche nella dottrina italiana si sottolinea il successo dei *VORP* nel dare spazio alle istanze delle vittime soprattutto nei casi di piccola criminalità e di delinquenza minorile, per i quali l'incontro tra l'autore e la persona offesa ha maggiori possibilità di esito positivo[47]. La prima condizione del percorso di mediazione è il riconoscimento della sofferenza della vittima e la consapevolezza delle proprie azioni delittuose da parte del reo[48].

44 Fiandaca, Musco 2024: 770.

45 Di Tommaso 2023: 42.

46 Di Tommaso 2023: 32; Mannozzi 2003: 20; Ruggeri 1985: 538; Lemert 1971; Bertolini 2015: 47 ss.; sulla diversione processuale per le persone giuridiche, v. Mazzacuva 2016: 80 ss.; Mangiaracina 2018: 2182*;* si veda anche Luparia 2015: 4; Greenblum 2005: 1866-1867; Garrett 2014: 55.

47 Di Tommaso 2023: 36;

48 Mannozzi 2003: *passim*; Id. 2023: 4; Di Tommaso, *ibidem*; Cingari 2023: 4.

Entrare in rapporto con l'offesa patita conduce alla riparazione del danno nella sua interezza. Proprio per il suo ruolo attivo nella riparazione, un terzo obiettivo è l'autoresponsabilizzazione del reo, che rimane protagonista della gestione del conflitto derivante dal reato. Sul piano sociale, l'evento criminoso diventa l'occasione per attivare una responsabilizzazione della comunità, che consente di rafforzare gli *standards* di comportamento e diminuire la percezione di insicurezza.

Nel nostro ordinamento, la mediazione e la riparazione alle vittime di reato hanno ricevuto una prima generale regolamentazione nel D.lgs. 274/2000, dedicato alla competenza del Giudice di Pace, al fine di favorire una composizione bonaria dei conflitti. Si trattò della prima legge orientata alla mediazione come modalità di risoluzione dei conflitti ed alla riparazione come meccanismo estintivo del reato. Peraltro, come dimostrato dalla limitazione dell'art. 29 ai soli reati perseguibili a querela di competenza del Giudice di Pace, il legislatore ha in quella sede individuato come prototipo del reato mediabile alcune fattispecie espressione di microconflittualità, costruite su un evento di danno di lieve entità. Un secondo istituto riconducibile al paradigma riparativo è previsto dall'articolo 35 del D.lgs. 274/2000, che fa riferimento alla condotta riparativa posta in essere prima del giudizio come causa di estinzione del reato. Nel più ristretto ambito della giustizia minorile, già il D.P.R. 448/1988 aveva introdotto all'art. 28 un istituto, la sospensione del procedimento con messa alla prova, comportante l'esecuzione di un programma trattamentale e di riparazione ed eliminazione delle conseguenze del reato, comportante, in caso di esito positivo, l'estinzione del reato. Proprio il favorevole riscontro ricevuto ne ha comportato, con la l. 67/2014, l'estensione anche nel contesto del processo penale agli adulti, i quali, in caso di reati particolarmente gravi, possono richiedere la sospensione con messa alla prova e ricorrere altresì alla mediazione penale con la persona offesa[49].

In tempi più recenti, merita di essere citato l'art.162 *ter* cp., coniato dalla legge 103/2017, che per la sua collocazione nella parte generale del codice penale assume un significativo rilievo sistematico.

La disposizione in commento prevede l'estinzione del reato, nei casi di procedibilità a querela, sentite le parti e la persona offesa, quando l'imputato ripari interamente, entro la dichiarazione di apertura del dibattimento di primo grado, il danno cagionato dal reato.

Una disciplina più organica della giustizia riparativa, anche per effetto degli impulsi di fonte sovranazionale[50], è stata introdotta dal D.lgs. 150/2022, che ha rego-

49 I dati forniti dal Dipartimento per la Giustizia Minorile, consultabili all'indirizzo https://www.giustizia.it, relativi proprio all'applicazione della mediazione penale ai soggetti di minore età, mostrano che, nonostante una tendenza al blocco della mediazione nella fase iniziale, una volta avviato sussiste per i minori un'elevata possibilità di conclusione positiva del percorso. Nel periodo 1992-2021, si è evidenziato un ricorso quadruplicato alla mediazione, con esiti positivi attestati attorno all'80%. Un commento ai numeri citati si deve a Di Tommaso, 2023 109 ss.

50 Si fa riferimento, in particolare, alla Raccomandazione del Comitato dei Ministri del Consiglio d'Europa agli Stati membri CM/Rec (2018)8 concernente la giustizia riparativa in materia penale, adottata il 3 ottobre 2018. Sulla genesi della *restorative justice* in Europa, cfr. Pali, Marder, 2024: 3-23.

lato l'innesto della stessa nel processo penale, in una logica di complementarità[51]. I programmi esperibili comprendono la mediazione tra autore e persona offesa, il dialogo riparativo e ogni altro programma dialogico guidato da mediatori, svolto nell'interesse della vittima e della persona imputata. Il decreto precisa che gli strumenti di giustizia riparativa sono accessibili in relazione a ogni tipo di reato, senza preclusioni legate alla sua gravità, e in ogni stato e grado del procedimento penale, nonché nella fase di esecuzione. Come si è efficacemente osservato, si tratta di una filosofia di maggiore apertura rispetto al passato[52], L'esito della mediazione o del programma è valutato dal giudice, in vista di una possibile definizione favorevole del processo; in ogni caso, il mancato raggiungimento dello scopo riparativo non può produrre effetti sfavorevoli per l'autore del reato.

Ciò premesso, si vuole evidenziare come, a fronte degli effetti devastanti per la persona di alcuni reati commessi in rete, un modello retributivo, inteso a raddoppiare l'afflizione del colpevole si dimostra insufficiente. Invero, anche la pena più severa non può sanare i gravi abusi subiti dalle vittime, e rischia di apparire meramente simbolica, in assenza di misure di protezione della vittima e di una più ampia opera di orientamento culturale[53].

Ma anche dall'angolo prospettico del reo, un tale approccio non favorisce una comprensione del danno arrecato né un'identificazione empatica con le vittime, ma, consolidandone l'esclusione sociale, pregiudica le possibilità di reinserimento nella comunità[54]. Dietro l'autore di un reato informatico sovente si cela non un pericoloso "nemico" dell'ordinamento, ma un utente da rieducare, in quanto non del tutto consapevole delle potenzialità lesive del *web*, o persino minorenne, per il quale un approccio incentrato sulla sola pena detentiva incentiverebbe nuove pulsioni criminogene.

L'ampiezza del dato normativo consente oggi di ipotizzare un maggiore ricorso alla mediazione, in particolare nelle ipotesi in cui vi è l'esigenza di riparare la sofferenza in cui si concreta l'offesa alle vittime, e vi sia la possibilità di instaurare, ovvero di ripristinare, un dialogo tra vittima e autore del reato, al fine di favorire in quest'ultimo una consapevolezza delle conseguenze e del disvalore della propria condotta.

Un valido esempio dell'opportunità di affiancare altri strumenti alla pena tradizionalmente intesa può essere costituito dalle fattispecie riconducibili alle categorie della pornografia non consensuale, del *cyberstalking* e del cyberbullismo, ove a vario titolo si realizza, grazie alle moderne tecnologie, una vera e propria invasione della sfera intima della persona, con pregiudizio per la sua riservatezza e dignità[55].

51 Per un commento alla riforma, v. Ceretti, Mannozzi, Mazzucato 2024: 59 ss.; Fiandaca, Musco 2024: 770 ss.; Mannozzi 2023: 649 ss.; Di Tommaso 2023; Insolera 2023; Gatta 2021; Palazzo 2022; Cingari 2023: 1 ss.

52 Mannozzi 2024: 83.

53 Per una riflessione sui rischi dell'uso simbolico del diritto penale, con riferimento alla pornografia virtuale, si veda Beguinot 2023: 29; l'autrice cita anche la raccolta in atti del dibattito promosso dall'Aipdp 2016; sul tema, v. altresì Moccia, 1992: 109.

54 Duff 1991: 239 ss; Visconti 2018: 47; Maugeri 2020: 29.

55 Sulla pornografia virtuale, cfr., in particolare, Helfer, 2007: 7; Caletti, 2018: 77; in relazione al concetto di ubiquità delle immagini personali, v. McGlynn, Rackley 2017: 535; Adamo

In particolare, il cyberbullismo costituisce un fenomeno ampio che può concretizzarsi, rispettivamente, in fatti di minaccia, diffamazione, estorsione, trattamento illecito di dati e, nei casi più gravi, di istigazione al suicidio. In questa materia si è affermato un mutamento di prospettiva, attraverso un approccio multidisciplinare, comprensivo di rimedi preventivi, riparatori, rieducativi e parapenali, che richiedono il coinvolgimento anche degli organi istituzionali e della società civile.

Può farsi riferimento, in primo luogo, alla principale forma di tutela della persona offesa, prevista dall'art. 2 della l. 71/2017, ossia la possibilità di inoltrare un'istanza al titolare del trattamento o al gestore del sito *internet* per ottenere la rimozione dei dati diffusi in rete. In secondo luogo, deve essere sottolineata l'emersione di prassi e protocolli improntati alla logica riparativa, come l'intesa stipulata dalla Procura della Repubblica presso il Tribunale per i Minori di Milano con il Comune ed il Centro per la Giustizia Riparativa e la Mediazione Penale che, per reati ricollegabili per lo più nelle fasce di età dei minori e dei giovani adulti, dal *cyber bulling* agli altri usi illeciti della rete, incoraggia gli incontri tra la vittima e il reo e il compimento da parte di quest'ultimo di attività riparative[56].

La spinta verso una maggiore centralità delle vittime, alla base della *restorative justice*, è dovuta ad una nuova dimensione delle stesse non come entità astratte, il cui ruolo e le cui esigenze si esauriscono all'interno del processo, bensì come individui concreti portatori di istanze a partire dal diritto all'ascolto. Al contempo, l'emersione di principi solidaristici, grazie anche alle moderne costituzioni, insieme con la presa d'atto che determinate forme di criminalità accentuano la vulnerabilità di alcune categorie di soggetti, suscita nella collettività, unitamente all'esigenza della pena, anche una spinta alla riparazione. Alla luce di quanto affermato, la mediazione può rappresentare uno strumento moderno per affrontare le complesse dinamiche criminose scaturenti dalle interazioni sociali nelle società interconnesse grazie alla globalizzazione[57].

Tuttavia, una riflessione sulla giustizia riparativa non può esimersi dal rilevare le criticità, espresse in dottrina, di un'adesione acritica a tale paradigma. In primo luogo, si è evidenziato l'atteggiamento prudente del legislatore della riforma sul piano degli effetti favorevoli conseguibili dal reo per effetto della spontanea partecipazione a programmi riparativi[58]. Ad eccezione di casi marginali di reati punibili a querela, quest'ultimo potrà beneficiare non di una completa non punibilità so-

2004; sul *cyberstalking*, figura che comprende diverse fattispecie di reato, v. Macrì 2019: 615-631; sulla fattispecie di cyberbullismo, v. Parmiggiani 2019: 631-656.

56 Il "*Progetto legalità*", ispirato alle direttive europee in tema di attenzione alla vittima ed alle migliori pratiche di mediazione penale e di attività riparative costituisce uno dei primi riferimenti a livello nazionale. Il tema è stato oggetto, in data 2 dicembre 2016, di una Tavola rotonda, intitolata: "*Il coinvolgimento del Minore – quale autore e quale vittima – nei reati informatici*", con la partecipazione della Procura della Repubblica, del Comune e delle Camere Penali Minorili di Milano. Questa sinergia si è tradotta anche nell'elaborazione di alcune linee guida, consultabili al link https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803060a7

57 In particolare, Palazzo, Bartoli 2011: 35, scorgono in questo rimedio un'utile modalità di gestione dei conflitti nelle societa globalizzate, che si connotano per un sempre più spiccato pluralismo valoriale.

58 Fiandaca, Musco 2024: 773.

pravvenuta, ma di un'attenuazione della pena *ex* art. 133 c.p., dell'accesso a misure alternative alla detenzione o della sospensione della pena, ciò che rappresenta un possibile disincentivo alla disponibilità ad un percorso di mediazione.

In secondo luogo, sono state sollevate riserve sul generico concetto di esito riparativo, definito come "qualunque accordo, risultante dal programma di giustizia riparativa, volto alla riparazione dell'offesa e idoneo a rappresentare l'avvenuto riconoscimento reciproco e la possibilità di ricostruire la relazione tra i partecipanti"[59]. Sia pure in un'ottica di *favor rei*, questi concetti elastici consegnano al giudice un'ampia discrezionalità valutativa, che presuppone una consolidata cultura della riparazione.

Alcuni rilievi sono stati posti anche sul concetto stesso di idoneità dell'accordo a "rappresentare l'avvenuto riconoscimento reciproco e la possibilità di ricostruire la relazione tra i partecipanti". Si osserva, in primo luogo, che la necessità di ricostituire un simile rapporto non è concepibile per tutti i reati; in secondo luogo, si rileva che non dovrebbe considerarsi preclusa la riparazione solo perché l'autore del reato, disponibile a reintegrare il bene leso, non sia intenzionato ad instaurare un dialogo con la parte offesa, in quanto non sarebbe compito di uno Stato liberale e democratico inculcare nei cittadini adulti una particolare concezione dei rapporti sociali[60]. In tal senso, si segnala il rischio di sovrapporre il principio costituzionale di rieducazione, inteso come riacquisita attitudine al rispetto della legalità esteriore, con le considerazioni inerenti ai presupposti della riparazione[61]. Ancora, nonostante la scelta del D.lgs. 150/2022 di rendere accessibile la *restorative justice* per ogni tipo di reato, si ravvisano dei limiti oggettivi all'effettiva riparabilità di taluni gravi delitti – come l'omicidio, le stragi e gli attentati contro la pubblica incolumità – e di numerose fattispecie prive di un concreto impatto dannoso o pericoloso, configurate come reati di pericolo astratto o senza vittime. Rispetto a tali tipologie criminose sembra concepibile una riparazione solo simbolica; lo stesso decreto, all'art. 56, indica genericamente come modalità riparatorie immateriali le dichiarazioni o scuse formali e gli impegni comportamentali rivolti alla comunità[62]. Sotto tale profilo, la valutazione giudiziale sul valore sintomatico a favore del reo di simili modalità riparatorie si preannuncia opinabile, specie se raffrontata al giudizio sulle condotte materialmente riparatrici esperibili per altre fattispecie.

Secondo questa condivisibile ricostruzione, la giustizia riparativa può trovare spazio in funzione complementare e non di alternatività alla giustizia punitiva tradizionale, difettando di un'adeguata risposta general-preventiva per le forme di criminalità più gravi e di maggior allarme sociale[63]. Si tratta di un modello più

59 Fiandaca, Musco 2024: 771.

60 Fiandaca, Musco 2024, 772.

61 In particolare, Fiandaca 2020: 5, avverte dal rischio di identificazione e ibridazione di concetti dai confini fluidi, come quelli di riparazione, rieducazione e risocializzazione.

62 Pagliaro 2020: 833 e 834; Fiandaca Musco 2024: 773; Insolera 2023: 10. Tuttavia, la giurisprudenza di merito sembra aprire al percorso di riparazione anche nell'ipotesi di vittima "surrogata" o "aspecifica" per gravi reati, v. Corte d'Assise di Busto Arsizio, ord. 19 settembre 2023, con commento critico di Maggio, Parisi 2023.

63 Insolera 2023: 10; Fiandaca, Musco 2024: 770;

efficace se applicato a taluni tipi di autori, come i minori, ed a reati che, per il minor allarme sociale che determinano, meglio si prestano ad una sostituzione della pena[64]. Per citare Garapon, una dimensione speciale della giustizia riparativa può ravvisarsi in quei fatti che non sono riconducibili ad una risposta reintegratoria attraverso la giustizia convenzionale e nei quali è necessario riaffermare e riconoscere la sofferenza dell'individuo[65]. Estendere il modello del "delitto riparato" oltre i confini di una complementarietà limitata ad alcune tipologie di autori e di incriminazioni si tradurrebbe in un'eterogenesi dei fini, in una privatizzazione dello *jus puniendi* sottratto allo Stato di diritto e plasmato sulle istanze e sulle pulsioni delle vittime e della collettività[66].

Lo stesso può garantire ottimi risultati nei casi in cui vi è uno spazio per una reintegrazione dell'offesa patita dalle vittime, ma si preannuncia di più difficile praticabilità per le categorie di macrocriminalità organizzata o terroristica che agiscono nel cyberspazio, ovvero per gravi e irreparabili episodi di istigazione al suicidio.

Sia pure con la cautela professata da autorevole dottrina, la giustizia riparativa, nella più ampia dimensione prospettata dalla riforma Cartabia, presenta delle potenzialità notevoli, in termini di ascolto delle vittime, di auto-responsabilizzazione del reo e di perseguimento di finalità special-preventive, mediante l'incisione degli specifici fattori criminogenetici che possono emergere nel percorso di mediazione, per contribuire ad un superamento culturale dei modelli di comportamento illeciti veicolati da *internet,* secondo il principio della pena come *extrema ratio*.

Bibliografia

Adamo, P., 2004, *Il porno di massa,* Milano: Raffaello Cortina Editore.

Aipdp, 2016, "La società punitiva. Populismo, diritto penale e ruolo del penalista", in *Diritto penale contemporaneo*.

Ayres, I., Braithwaite, J., 1992, *Responsive regulation: Trascending the Deregulation Debate*: 101 ss.

Bamberger, K. A., 2006, "Regulation as Delegation: Private firms, decision-making, and accountability in the administrative state", in 56 *Duke Law Journal* 377: 386.

Barmore, C., 2015, "Criminalization in Context: Involuntariness, Obscenity, and First Amendment", in *Stanford Law Review*, vol. 67: 447-478.

Baumann Z., 1990 *Modernità liquida*, Milano: Laterza.

Beguinot, G.., 2023 "I reati contro la sfera sessuale della persona al tempi di internet, tra criticità tradizionali ed esigenze di prevenzione", in *Rivista Italiana di Diritto e Procedura Penale*, fasc.3: 29.

64 Insolera *Ibidem*.

65 Garapon 2022.

66 Insolera 2023: 17; Pavarini 2013: 162, che, in una prospettiva ottimistica, definisce la *restorative justice* "*un porto in cui fare momentaneamente sosta*", mentre, in una prospettiva pessimistica, paventa il rischio di una privatizzazione del conflitto criminale. Per una ricostruzione del modello del delitto riparato, cfr. Donini 2020; Pulitanò 2020 e Fiandaca 2020: 2, ritengono incompleto un paradigma punitivo fondato esclusivamente sul modello in esame.

Bertagna, G., Ceretti, A., Mazzucato, C., 2015, *Il libro dell'incontro. Vittime e responsabili della lotta armata a confronto*, Milano: Il saggiatore.
Bertolini, B., 2015, "Esistono autentiche forme di "diversione" nell'ordinamento processuale italiano? Primi spunti per una riflessione", in *Diritto Penale Contemporaneo*, 4: 47ss.
Brenner, S.W., 2006, "Defining Cybercrime: A review of Federal and State Law", in R.D. Clifford (ed.), 2006, *Cybercrime: The investigation, prosecution, and defense of a computer-related crime*, Durham: Carolina Academic Pres.: 17.
Brunelli, D., 2019, *Il diritto penale delle fattispecie criminose. Strumenti e percorsi per uno studio avanzato*, Torino: Giappichelli: 46.
Brunelli, D., 2000, *Il reato portato a conseguenze ulteriori. Problemi di qualificazione giuridica*, Torino: Giappichelli.
Cadoppi A., Canestrari, S., Manna, A., Papa, M., 2019, *Cybercrime*, II Ed., Torino: Utet.
Cafaggi, F., 2012, "Enforcing transnational private regulation: models and patterns", in *Enforcement of Transnational Regulation. Ensuring Compliance in a Global World,* a cura di F. Cafaggi, Cheltenham: Edward Elgar: 75 ss.
Caldwell, F., 2020, *Governance, Risk and compliance. Improve Performance, reduce Uncertainties and optimize Grc Technologies*, Londra: Kogan.
Caletti, G.M., 2018, "Revenge Porn e tutela penale", in *Diritto Penale Contemporane*o, n. 3/2018: 81.
Carrara, M. 1874, *Momento consumativo del furto*, in *Lineamenti di pratica legislativa penale*, Torino: Giappichelli, 229 ss.
Cassese, S., 2009, *Il diritto globale. Giustizia e democrazia oltre lo Stato*, Torino: Einaudi, 142 ss.
Ceretti, A., Mannozzi, G., Mazzucato, C., 2024, *La disciplina organica della giustizia riparativa*, Torino: Giappichelli, 59 ss.
Cingari, F., 2023, "La giustizia riparativa nella riforma Cartabia", in *Sistema Penale*, 5 dicembre 2023.
Citron, D. K., Franks, M. A., 2014, "Criminalizing Revenge Porn", in *Wake Forest Law Review*, vol. 49: 345-391.
Clough, J., 2015, *Principles of cybercrime, second edition,* Cambridge: Cambridge University Press: 11 ss.
Cocco, G., 2006, "Può costituire reato la detenzione di pornografia minorile", in *Rivista italiana di diritto e procedura penale,* 3: 863 ss.
Cocco, G., 2018, "Teorie sulla pena e applicazione pratica", in G. Cocco, E. Ambrosetti (a cura di), *Trattato breve di diritto penale. Parte generale – II. Punibilità e pene*, Milano: Cedam:14 ss.
Colacurci, M., 2022, *L'illecito "riparato" dell'ente,* Torino: Giappichelli, 75.
Corbella, S., Pozza, L., 2016, "Modello 231 e sistema di controllo interno: aree di sovrapposizione e profili di differenziazione. Implicazioni in termini di costi e benefici sull'assetto degli organi di controllo e vigilanza", in F. Centonze, M. Mantovani (a cura di), *La responsabilità penale degli enti. Dieci proposte di riforma*, Bologna: Il Mulino, 52 ss.
Cornacchia, L., 2010, "Tutela di beni giuridici versus tutela di norme", in S. Vinciguerra, F. Dassano (a cura di), *Studi in memoria di Giuliano Marini*, Napoli: Jovene, 220 ss.
Cornacchia, L., 2012, *La vittima nel diritto penale contemporaneo tra paternalismo e legittimazione del potere coercitivo*, Roma: Aracne.
Di Martino, A., 2010, *Il territorio: dallo stato-nazione alla globalizzazione. Sfide e prospettive dello stato costituzionale aperto*, Milano: Giuffrè, 74 ss.

Di Tommaso, G., 2023, *La giustizia riparativa dagli albori alla riforma Cartabia*, Milano: Franco Angeli.
Donini, M., 2011, *Europeismo giudiziario e scienza penale. Dalla dogmatica classica alla giurisprudenza-fonte*, Milano: Giuffrè, 46 ss.
Donini, M., 2020, "Pena agita e pena subita. Il modello del delitto riparato", in www.questionegiustizia.it, 29 ottobre 2020.
Donini, M., 2013, "Per una concezione postriparatoria della pena. Contro la pena come raddoppio del male", in *Rivista italiana di diritto e procedura penale*, 1162 ss.
Duff, R.A.1991, „Punishment, Expression and Penance", in Jung, H. Muller-Dietz, H. Neumann, U., *Recht und Moral: Beitrage zu einer Standortbestimmung*, Baden-Baden, 239 ss.
Eusebi, L., 2001, "Politica criminale e riforma del diritto penale", in S. Anastasia, M. Palma (a cura di), *La bilancia e la misura. Giustizia, sicurezza e riforme*, Roma: FrancoAngeli.
Ferrarese, M. R., 2012, *Prima lezione di diritto globale*, Roma: Universale Laterza.
Fiandaca, G., "Note su punizione, riparazione e scienza penalistica", in *Sistema Penale*, 9 novembre 2020.
Fiandaca, G., Musco, E., 2024, *Diritto Penale. Parte Generale*, Nona Edizione, Bologna: Zanichelli.
Fiandaca, G., Visconti, C. (a cura di), 2009, *Punire mediare riconciliare. Dalla giustizia penale internazionale all'elaborazione dei conflitti individuali*, Torino: Giappichelli.
Fiandaca, G., 1982, "Il "bene giuridico" come problema teorico e come criterio di politica criminale", *Rivista Italiana di Diritto e procedura penale*, 42 ss.
Fiorella A. (a cura di), 2012, *Corporate criminal liability and compliance programs. Vol. 1: Liability "ex crimine" of legal entities in Member States*, Napoli: Jovene, 14 ss.
Fiorella, A., Selvaggi, N., 2018, *Dall'"utile" al "giusto": il futuro dell'illecito da reato dell'ente nello "spazio globale"*, Torino: Giappichelli, 12.
Flor R., 2019, "La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative", in A. Cadoppi, S. Canestrari, A. Manna, S. Papa, *Cybercrime*, Milano: Utet: 75.
Garapon, A., 2022, "Justice caught between being and having", in *The International journal of restorative justice*, 08/01 https://www.elevenjournals.com.
Garrett, K. 2014, *Too Big to Jail. How Prosecutors Compromise with Corporations*, The Belknap Press of Harvard University Press: 55.
Gatta, G.L., 2021, "Riforma della giustizia penale: contesto, obiettivi e linee di fondo della 'legge Cartabia'", in *Sistema penale,* 15 ottobre 2021.
Gibbs, J. L., 1963, "The Kpelle Moot: A Therapeutic Model for the Informal Settlement of Disputes", in *Africa*, Volume 33 (1): 1-11 – Jan 1.
Gillespie, A. A., 2016, *Cybercrime. Key Issues and Debates,* Abingdon-New York: Routledge.
Giorgino, M., Pozza, L., 2017, "Compliance e rischi aziendali", in G. Rossi (a cura di), *La corporate governance: una nuova frontiera per il diritto?*, Milano: Giuffrè:103 ss.
Gobert, J., Punch, M., 2003, *Rethinking corporate crime*, Cambridge: Cambridge University Press, 315 ss.
Gulliver, P.H., 1969, "Dispute settlement without courts: The Ndendeuli of Southern Tanzania", in L. Nader (a cura di), *Law in Culture and Society*, Chicago: Aldine Publishing.
Greenblum, B.M., 2005, "What Happens to a Prosecution Deferred – Judicial Oversight of Corporate Deferred Prosecution Agreements", in *Columbia Law Review*, 105: 1866-1867.
Gullo, A., 2021, "I modelli organizzativi", in G. Lattanzi, L., Severino, *Responsabilità da reato degli enti. Volume I Diritto Sostanziale*, Torino: Giappichelli, 245.

Helfer, M., 2007, *Sulla repressione della prostituzione e pornografia minorile. Una ricerca comparatistica*, Padova: Cedam: 7.
Hoffe, O., 2001, *Globalizzazione e diritto penale*, Torino: Giappichelli.
Hellmer J., 1972, „Massenkriminalität" (Begriff, Wesen, Konsequenzen), in AA.VV., *Zum Phänomen der Massenkriminalität und zu den Möglichkeiten ihrer Bekämpfung,* Polizei-Institut, 1972: 21ss.
Ingrassia A., 2012, "Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano", in *Diritto Penale Contemporaneo*, 8 novembre, 2.
Insolera, G., 2023, *Sulla giustizia riparativa*, Napoli: Editoriale Scientifica.
Jescheck, H., Weigend, T., 1996, *Lehrbuch des Strafrechts. Allgemeiner Teil*, 5, Aufl., Berlino: Dunker & Humblot.
Kamal, M., Newman, W. J., 2016, "Revenge Pornography: Mental Health Implications and Related Legislation", in *The Journal of American Academy of Psychiatry and the Law*, vol. 44, n. 3: 359-367.
Kumar Sen, A., 2009, *L'idea di giustizia,* Milano: Mondadori.
Lamanuzzi, M., 2015, "Vulnerabilità e predisposizioni vittimologiche: una politica criminale più sensibile alle vittime deboli", in M.F., Cortesi, E. La Rosa, L. Parlato, N. Selvaggi (eds.), *Sistema penale e tutela delle vittime tra diritto e giustizia*, Milano: Diplap, 31 ss.
Larkin, P. J., 2014, "Revenge Porn, State Law and Free Speech", in *Loyola of Los Angeles Law Review*, vol. 48, 62 ss.
Lemert, E. M., 1971, *Instead of Court. Diversion in juvenile justice*, Washington: U.S. Government Printing Office.
Lubman, S., 1967, "Mao and mediation: politics and dispute resolution in Communist China", in *California Law Rev*. 55: 1284-1359.
Luparia, L., 2015, "Contrasto alla criminalità economica e ruolo del processo penale: orizzonti comparativi e vedute nazionali*",* in *Processo Penale e Giustizia*, n. 5, 4.
Macrì, F., 2019, "Il cyberstalking", in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Milano: Utet, 615-631.
Maggio, P., Parisi, F., 2023, "Giustizia riparativa con vittima "surrogata" o "aspecifica": il caso Maltesi-Fontana continua a far discutere", *Sistema Penale*, 19 ottobre.
Mangiaracina, A., 2018, "Persone giuridiche e alternative al processo: I deferred prosecution agreements nel Regno Unito e in Francia", in *Cassazione Penale.*, n. 6, 2182.
Manna, A., 2010, "I soggetti in posizione di garanzia", in *Diritto informazione e informatica*, 6, 2010.
Manna, A., Di Fiorio, M., 2019, "Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissionem dell'internet service provider", in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Cybercrime, Milano: Utet, 891 ss.
Mannozzi, G., 2003, *La giustizia senza spada. Uno studio comparato su giustizia riparativa e mediazione penale*, Milano: Giuffrè.
Mannozzi, G. 2024, "Definizioni, principi generali, obiettivi e ambito di applicazione della giustizia riparativa", in Ceretti, A., Mannozzi, G., Mazzucato, C., 2024, *La disciplina organica della giustizia riparativa*, Torino: Giappichelli, 75-92.
Mannozzi, G., Lodigiani, G. A. (a cura di), 2015, *Giustizia riparativa. Ricostruire legami ricostruire persone*, Bologna: Il Mulino.
Mannozzi, G., 2023, "La giustizia riparativa: brevi note su contesto, disciplina ed effetti trasformativi", in *Rivista Italiana di Diritto e Procedura Penale*, fasc.2, 1 giugno: 649.
Marinucci, G., Dolcini, E. Gatta, G. L., 2019, *Manuale di diritto penale*, Milano: Giuffrè, 257 ss.

Marinucci, G. 2009, "Causalità reale e causalità ipotetica nell'omissione impropria", *Rivista Italiana di Diritto e Procedura Penale*, 523 ss.
Maugeri, A., 2020, "Diritto penale del nemico e reati sessualmente connotati", in *Rivista Italiana di Diritto e Procedura Penale*, fasc.2, 1 giugno: 29.
Mazzacuva, F., 2016, "La diversione processuale degli enti collettivi nell'esperienza angloamericana. Alcuni spunti de jure condendo", in *Diritto Penale Contemporaneo*, 2/2016: 80 ss.
McGlynn C., Rackley, E., 2017, "Image-Based Sexual Abuse", in *Oxford Journal of Legal Studies*, vol. 37, n. 3: 535.
Miller, G.P., 2017, "Compliance: Past, present and future", 48 *U. Tol L. Rev*.: 446.
Moccia, S., 1992, *Il diritto penale tra essere e valore. Funzione della pena e sistematica teleologica*, Napoli: Edizioni Scientifiche Italiane, 109.
Padovani, T., 2019, "L'assenza di coerenza mette a rischio la tenuta del sistema", in *Guida dir*., n. 37, 51.
Pagliaro, A., 1985, "Verifica empirica dell'effetto di prevenzione generale", in *Rivista italiana di diritto e procedura penale*: 353 ss.
Pagliaro, A., 2020, *Principi di diritto penale, parte generale*, Milano: Giuffrè.
Palazzo, F., Bartoli, R., 2011, *La mediazione penale nel diritto italiano e internazionale*, Firenze: Firenze University Press, 35.
Paliero, C.E., 1992, "Consenso sociale e diritto penale", in *Rivista italiana di diritto e procedura penale*.
Palazzo, F., 2022, "Plaidoyer per la giustizia riparativa", in www.*legislazionepenale.eu,* 31 dicembre.
Pali, B., Marder, I. D., 2024, "*Genesi ed evoluzione della giustizia riparativa in Europa*", in A. Ceretti, G. Mannozzi, C. Mazzucato, *La disciplina organica della giustizia riparativa*, Torino: Giappichelli, 3-23.
Paliero, C.E., 1985 «Minima non curat praetor». *Ipertrofia del diritto penale e decriminalizzazione dei reati bagatellari*, Padova: Cedam, 181 ss.
Paliero, C.E., 2014, "Il diritto liquido. Pensieri post-delmasiani sulla dialettica delle fonti penali", in *Rivista italiana di diritto e procedura penale*, 1129 ss.
Parmiggiani, M.C., 2019, "Il cyberbullismo", in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Milano: Utet, 631-656.
Parziale, Y., 2020, "Il ruolo della vittima del reato tra diritto e neuroscienze. Il caso dei minori", in *Cassazione Penale*, fasc.5, 1 maggio, 10.
Pavarini M., 2013, *Governare la penalità. Struttura sociale processi decisionali e discorsi pubblici*, ius17unibo.it, n. 3/2013, *Ai margini della penalità nella crisi della penalità*: 162.
Pecorella C., 2006, *Diritto penale dell'informatica*, Padova: Cedam.
Picotti L., 2000, "Reati informatici", in *Enc. Treccani*, Roma: Treccani.
Picotti, L., 2007, "I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici", in G. Forti, M. Bertolino, (eds): *Scritti per Federico Stella,* Napoli: Jovene, 1267-1322.
Picotti, L. 2011, "Sicurezza, informatica e diritto penale", in M. Donini, M. Pavarini, *Sicurezza e diritto penale*, Bologna: Bononia University Press, 217 ss.
Picotti L., 2019, "Diritto penale e tecnologie informatiche: una visione d'insieme", in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Milano: Utet, 75 ss.
Picotti L., 2004, "Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati", in Id., *Il diritto penale dell'informatica nell'epoca di Internet*, Padova: Cedam, 21ss.

Piergallini, C., 2010, "Globalizzazione dell'economia, rischio-reato e responsabilità ex crimine delle multinazionali", in *Rivista trimestrale di diritto penale dell'econonomia*, 1-2, 153.
Piergallini, C., 2015, "I delitti contro la riservatezza informatica", in C. Piergallini, F. Viganò, M. Vizzardi, A. Verri, *I delitti contro la persona*, Padova: Cedam, 769-789.
Piergallini, C., 2016, "Ius sibi imponere: controllo penale mediante autonormazione?" in C.E., Paliero, S. Moccia, G. De Francesco, G. Insolera, M. Pelissero, R. Rampioni, G. Riscato (a cura di), *La crisi della legalità. Il «sistema vivente» delle fonti penali*, Napoli: Jovene, 119 ss.
Power, M., 2004, *The risk-management of everything. Rethinking the politics of uncertainty*, Londra: Demos, 13 ss.
Pulitanò, D., 2020, "Il diritto penale tra teoria e politica", in *Sist. Pen*., 9 novembre.
Romano, M., 2004, *Commentario sistematico del codice penale*, I, 3° ed., Milano: Giuffrè, Pre-Art. 39: § 118s., 344 ss.
Ruggeri, F., 1985, "Diversion, dall'utopia sociologica al pragmatismo processuale", in *Cassazione Penale*: 538.
Schmitt, C., 1995, *Staat, Großraum, Nomos, Arbeiten aus den Jahren 1916-1969,* Berlino: Duncker & Humblot, 108 ss.
Sieber U., 2012 „Straftaten und Strafverfolgung", in *Internet, Gutachen Czum 69. Deutschen Juristentag*, Verlag C.H. Beck: Munchen: 18 ss.
Spagnoletti, V., 2004, "La responsabilità del provider per i contenuti illeciti in internet", in *Giur. mer.*, 1922 ss.
Venafro, E., 2004, "Brevi cenni introduttivi sull'evoluzione della tutela della vittima nel nostro sistema penale", in E. Venafro, C. Piemontese (a cura di), *Ruolo e tutela della vittima in diritto penale*, Torino: Giappichelli, 12.
Venturoli, M., 2015, *La vittima nel sistema penale dall'oblio al protagonismo?*, Napoli: Jovene, 8.
Venturoli, M., 2021, "La "centralizzazione" della vittima nel sistema penale contemporaneo tra impulsi sovranazionali e spinte populistiche", in *Archivio Penale*, n. 2, 1 ss.
Visconti, A., 2018: *Reputazione, Dignità, Onore, Confini penalistici e prospettive politico criminali*, Torino: Giappichelli, 47.
Weismann M. F., 2011, "International Cybercrime: Recent Developments in the Law", in R. D. Clifford (ed.), *Cybercrime*, III Ed., Carolina Academic Press.
Guidelines to figth cybercrimes and protect victims, elaborate dalla Procura della Repubblica presso il Tribunale di Milano, dall'ordine degli Avvocati e dal Comune di Milano, consultabili al link https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803060a7

Luigi Previti

Convergenze e deviazioni in materia di cybersicurezza: implicazioni sistematiche e nuovi interrogativi

Abstract: Il lavoro si propone di evidenziare come le politiche italiane ed europee sulla cybersecurity, dopo una prima fase di disallineamento, stiano iniziando a convergere verso una visione unitaria dei rischi di cybersecurity e delle relative azioni da intraprendere, tra cui, in particolare, un più diretto e strutturato coinvolgimento del settore privato, al fine di raggiungere effettivamente un soddisfacente livello di cyber resilienza e cyber difesa. Tuttavia, l'attuazione delle linee strategiche definite a livello europeo, in parte recepite nella recente strategia italiana 2022-2026, solleva nuovi interrogativi teorici e questioni operative, che il contributo cerca di individuare, a partire da un ripensamento generale del ruolo dello Stato in questo delicato settore.

Keywords: Cybersecurity; Strategia europea; Strategia italiana; Partenariato pubblico-privato; Regolazione di mercato.

1. Premessa

Negli ultimi anni il sistema italiano di tutela della sicurezza cibernetica sta attraversando un importante processo di trasformazione e adeguamento.

La sua articolazione originaria, che faceva capo, principalmente, alle diverse strutture amministrative attive nel c.d. "Sistema di informazione per la sicurezza della Repubblica"[1], è stata incisivamente modificata, com'è noto, a seguito dell'entrata in vigore di due significativi interventi normativi.

Il primo è rappresentato dal d.l. 21 settembre 2019, n. 105, conv. dalla l. 18 novembre 2019, n 133, che ha introdotto il Perimetro di Sicurezza Nazionale Cibernetica (di seguito, anche PSNC) al fine di garantire un livello elevato di sicurezza delle reti, dei dispositivi e dei servizi *online* utilizzati dai soggetti (pub-

1 Al riguardo, si vedano la l. 3 agosto 2007, n. 124, come modificata dalla l. 7 agosto 2012, n. 133, nonché i successivi DPCM del 24 gennaio 2013 e del 17 febbraio 2017, entrambi rubricati "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". Sul sistema delineato dalla l. n. 124/2007, cfr. Franchini 2010: 431 ss.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760163

bliche amministrazioni ed enti privati) che esercitano una funzione o un servizio "essenziale" dello Stato[2].

Il secondo è costituito, invece, dall'introduzione, ad opera del d.l. 14 giugno 2021, n. 82, conv. dalla l. 4 agosto 2021, n. 109, dell'Agenzia per la cybersicurezza nazionale (di seguito, ACN), quale punto di riferimento fondamentale per tutti i soggetti inseriti all'interno del Perimetro, "punto di contatto unico" transfrontaliero e principale centro di attuazione della politica nazionale in materia[3].

In particolare, spetta all'Agenzia esercitare un coacervo di rilevanti compiti istituzionali, che ricomprende, tra gli altri, la predisposizione e l'aggiornamento della strategia nazionale di cybersicurezza[4], l'ispezione, l'accertamento e l'irrogazione delle sanzioni prescritte in caso di violazioni della normativa di riferimento[5], il coordinamento e la direzione del sistema di certificazione, qualificazione e valutazione della cybersicurezza dei prodotti, servizi e processi ICT[6], il rafforzamento delle capacità e delle conoscenze nel settore[7], la gestione delle crisi informatiche e il monitoraggio del verificarsi di attacchi e incidenti *cyber*[8], la promozione di attività e progetti rivolti alla formazione e alla sensibilizzazione collettiva[9].

2 In particolare, tali soggetti sono tenuti ad adottare particolari precauzioni organizzative e tecniche, più consistenti rispetto a quelle adottate da altri enti, tra i quali rientrano: *i*) l'obbligo di aggiornare, con cadenza annuale, gli elenchi delle reti, dei sistemi e dei servizi informatici; *ii*) l'obbligo di compiere analisi di valutazione del rischio di eventuali interruzioni o danneggiamenti dei sistemi e delle reti usati per la propria attività; *iii*) l'obbligo di comunicare al Centro di Valutazione e Certificazione nazionale (CVCN) istituito presso l'ACN la volontà di acquistare beni e sistemi tecnologici sul mercato, in modo tale da accertarne l'affidabilità; *iv*) l'obbligo di rispettare gli oneri di segnalazione al CSIRT Italia, in caso di incidenti o di attacchi aventi un impatto rilevante. Sull'istituzione del PSNC, si vedano, tra gli altri, Carotti 2020: 629 ss.; Mele 2020: 186 ss.; Renzi 2021: 538 ss.

3 Sui peculiari caratteri strutturali e funzionali dell'ACN, cfr. Parona 2021: 713 ss.; Serini 2022: 241 ss.; Forgione 2022: 1113 ss.

4 Il testo della suddetta strategia nazionale, adottata per il quinquennio 2022-2026, è reperibile al sito www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza.

5 Funzioni che vengono ulteriormente potenziate e coordinate, da ultimo, a seguito dell'entrata in vigore della l. 28 giugno 2024, n. 90, rubricata "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", specie con riferimento agli obblighi di notifica degli incidenti *cyber*.

6 In quanto "Autorità nazionale di certificazione della cybersicurezza" ai sensi dell'art. 58 del regolamento UE 2019/881 del 17 aprile 2019, c.d. *Cybersecurity Act*, con il compito di attuare un controllo preventivo sulla sicurezza di tuti gli acquisti di beni e sistemi ICT che supportano la fornitura di servizi e funzioni essenziali a livello nazionale.

7 In quanto "Centro nazionale di coordinamento" ai sensi dell'art. 6 del regolamento UE 2021/887 del 20 maggio 2021, con il compito di supportare il Centro europeo di competenza per la cybersicurezza nell'attività di rafforzamento delle capacità, delle conoscenze e della competitività dell'Unione nel settore.

8 Presso l'ACN opera, infatti, lo CSIRT Italia, con il compito di ricevere le segnalazioni di eventuali incidenti o attacchi cibernetici, emettere allarmi e allerte, nonché offrire assistenza operativa in situazioni di crisi.

9 Tali attività vengono espletate anche tramite il coinvolgimento di università, enti di ricerca, imprese e altre istituzioni pubbliche.

I recenti assestamenti strutturali paiono aver conferito all'architettura italiana una forma maggiormente compatta e coordinata a livello funzionale, che risulta essere sempre più orientata a soddisfare le crescenti esigenze di celerità ed efficienza dell'azione di contrasto.

Tuttavia, se si rivolge attentamente lo sguardo alle caratteristiche e alla portata delle minacce della dimensione cibernetica[10], in cui anche l'utente medio o la piccola impresa possono rappresentare *target* appetibili per i criminali informatici[11], appare opportuno continuare a interrogarsi in merito all'adeguatezza e all'effettività delle misure e degli strumenti che connotano il complessivo sistema nazionale, in gran parte rivolti nei confronti dei gestori delle infrastrutture e dei servizi digitali di maggiore importanza per la vita del Paese[12].

La presente riflessione mira ad evidenziare il valore strategico del contributo svolto dal settore privato-imprenditoriale nel delicato contesto in esame. Nello specifico, dopo aver sottolineato le principali modalità attraverso le quali, sulla falsariga delle indicazioni europee, la preziosa cooperazione tra autorità istituzionali e imprese che operano nell'ambito delle *Information and Communication Technologies* (ICT) e della *cybersecurity* può concretamente esplicarsi, verranno illustrate le più recenti iniziative avviate in tal senso a livello nazionale. Tale disamina consentirà di svolgere, in seguito, alcune considerazioni di sintesi in merito alle implicazioni sistematiche e agli interrogativi teorici che la concreta attuazione dei citati indirizzi strategici non può che suscitare, a partire dal ripensamento del ruolo finora riservato ai poteri statali nell'affrontare le nuove sfide poste dalla sicurezza informatica.

2. Il contributo degli operatori economici privati nella visione europea di cyberspazio

Nonostante il tema della sicurezza informatica sia conosciuto e discusso da tempo[13], i primi tentativi di dettare una risposta uniforme a livello sovranazionale si

10 Si pensi, ad esempio, alla diffusione a livello internazionale di quei dispositivi che appartengono al vasto insieme dell'*Internet of Things,* quale fenomeno che sta determinando, rispetto al passato, un vertiginoso aumento delle superfici di attacco e del numero dei *target* colpiti. Si pensi, ancora, alla crescente espansione della c.d. economia cybercriminale, che ha visto fiorire nel tempo un vero e proprio mercato *online* (solitamente, nel *dark web)* di prodotti e servizi volti a consumare pericolosi attacchi informatici e offerti, a costi contenuti, anche a soggetti non particolarmente esperti nell'uso delle tecnologie, in aderenza al concetto del "*Crime as a Service*". In merito al concetto del "*Crime as a Service*", si veda Paganini 2022: 67 ss. Sulla criminalità informatica e sulle connesse problematiche di diritto penale, si rinvia, per tutti, ad Amato Mangiameli, Saraceni 2019.

11 Si pensi, al riguardo, ai sempre più frequenti attacchi informatici alla *supply chain*, rivolti nei confronti di imprese di piccole e medie dimensioni con il precipuo intento di colpire imprese di grandi dimensioni di cui sono fornitori. Sull'esigenza di intervenire per migliorare il livello di alfabetizzazione digitale e di consapevolezza degli utenti della rete, cfr. Montessoro 2019: 783 ss.; Ziccardi 2019: 210.

12 Al riguardo, cfr. anche Brighi, Chiara 2021: 20 ss.

13 Cfr., tra gli altri, la comunicazione della Commissione europea del 6 giugno 2001, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM

rintracciano soltanto di recente, segnatamente nell'ambito delle diverse iniziative dedicate alla realizzazione del *Digital Single Market*[14].

Con questi atti l'Unione ha inteso affermare, in particolare, una propria visione strategica del cyberspazio, quale luogo virtuale aperto e sicuro per lo svolgimento delle attività economiche e sociali dei cittadini europei, improntato alla protezione e all'affidabilità dei dati, delle reti e dei prodotti informatici presenti al suo interno. Un ambito dai confini indefiniti[15], del quale si intende garantire un elevato livello di resilienza tramite l'applicazione di politiche e misure omogenee, nonché tramite un efficiente meccanismo di segnalazione degli incidenti e degli attacchi più rilevanti[16].

Nei più recenti atti di indirizzo adottati in materia, che si occupano spesso di rimarcare come la sicurezza informatica costituisca il risultato dell'intervento attivo di diversi attori (pubblici e privati)[17], pare possibile notare lo sforzo delle istituzioni dell'Unione di promuovere un più diretto e articolato coinvolgimento del settore imprenditoriale all'interno dei sistemi di prevenzione e difesa elaborati dagli Stati membri.

Sotto questa prospettiva va notato, in primo luogo, come le imprese che producono, offrono o importano prodotti tecnologici nell'Unione siano chiamate ad assumere un impegno giuridicamente vincolante, fin dal momento della progettazione, all'interno del mercato unico.

(2001) 298; nonché la comunicazione della Commissione europea del 26 settembre 2003, *Il ruolo dell'e-Government per il futuro dell'Europa*, COM (2003) 567.

14 In materia, cfr. la comunicazione della Commissione europea del 6 maggio 2015, *Strategia per il mercato unico digitale in Europa*, COM (2015) 192 final, spec. par. 3.4; la direttiva UE 2016/1148 del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, c.d. direttiva NIS 1, modificata, da ultimo, dalla direttiva UE 2022/2555 del 14 dicembre 2022, c.d. direttiva NIS 2; le comunicazioni congiunte della Commissione europea e dell'Alto rappresentante dell'Unione, rispettivamente, del 7 febbraio 2013, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN (2013) 1 final, del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte dell'UE*, JOIN (2017) 450 final, e del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN (2020) 18 final; il regolamento UE 2019/881 del 17 aprile 2019, c.d. *Cybersecurity Act.*

15 Cfr. Rodotà 2014: 3, il quale ha definito il cyberspazio come "il più grande spazio pubblico che l'umanità abbia conosciuto".

16 Sulla visione strategica dell'Unione relativa allo spazio cibernetico, si vedano Contaldo, Mula 2020: 57 ss.; Kohler 2020: 7 ss.; Bassini 2021: 319 ss.; Baroni 2022: 373 ss.

17 Si vedano, ad esempio, la comunicazione della Commissione europea del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, par. 3.2, ove si afferma che: "La natura interconnessa del ciberspazio richiede che tutti i portatori di interessi si scambino informazioni e si assumano le proprie responsabilità specifiche, per mantenere un ciberspazio globale, aperto, stabile e sicuro", nonché la comunicazione della Commissione europea del 24 luglio 2020, *La strategia dell'UE per l'Unione della sicurezza*, COM (2020) 605 final, par. 3, ove si afferma che: "[…] la cooperazione con il settore privato è fondamentale, tanto più che l'industria possiede una parte importante dell'infrastruttura digitale e non digitale indispensabile per lottare efficacemente contro la criminalità e il terrorismo. Anche i singoli individui possono apportare il loro contributo, ad esempio creando competenze e consapevolezza per combattere la criminalità informatica o la disinformazione".

In tal senso, tali soggetti vengono obbligati, da un lato, a mettere in commercio esclusivamente beni e servizi che possiedono determinati requisiti di sicurezza contro il rischio di incidenti e di attacchi cibernetici (principio di *cybersecurity by design*); dall'altro, gli stessi sono chiamati a mantenere, nei confronti degli utenti, il ruolo di interlocutori principali durante l'intero ciclo di vita dei prodotti, collaborando con il settore pubblico nell'esercizio delle attività di controllo degli *standard* di sicurezza e assumendosi, di conseguenza, le relative responsabilità[18].

Da qui la previsione di una serie di peculiari oneri e adempimenti (verifiche *ex ante*, aggiornamenti costanti, revisioni periodiche, azioni mirate, interventi a tutela dei dati personali), tanto più stringenti quanto più elevati sono i rischi di manomissione delle applicazioni e dei dispositivi tecnologici offerti dalle imprese[19].

L'obiettivo di costruire un ecosistema *cyber* più efficiente e aperto si traduce, in secondo luogo, nella definizione di modalità più stabili e durature di cooperazione tra autorità pubbliche e settore privato, in grado di sfruttare adeguatamente le conoscenze e le capacità di analisi di quest'ultimo, "*that rival those of the world's most sophisticated intelligence agencies, including in the notoriously difficult task of attack attribution*"[20].

È sotto questa prospettiva che può essere compresa l'istituzione di alcune sedi privilegiate di raccordo di matrice europea, tra le quali: il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cybersicurezza, che intende sviluppare le risorse e le competenze dell'Unione e ridurre la sua dipendenza da Paesi terzi, impegnando le energie dei Centri nazionali di coordinamento (in Italia, l'ACN), del mondo dell'industria e delle università[21]; l'Unità congiunta per il cyberspazio (*Joint Cyber Unit*), quale piattaforma finalizzata a promuovere lo scambio di informazioni, buone pratiche e conoscenze, nonché la cooperazione tra le forze dell'ordine e della difesa, le autorità civili e diplomatiche e i privati interessati in caso di gravi attacchi o incidenti di natura transfrontaliera[22]; la rete dei Centri operativi di sicurezza (c.d. SOC, *Security Operations Center*), quale

18 In materia, cfr. anche Taddeo 2019: 351-352.

19 Il potenziamento degli obblighi e dei requisiti di sicurezza esigibili da parte dei produttori, importatori e distributori di prodotti digitali, già auspicato dalle comunicazioni congiunte del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'UE*, par. 2.2, e del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, par. 1.5., viene espressamente previsto dalla recente proposta di regolamento UE 2022/272 del 15 settembre 2022, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, COM (2022) 454 final, c.d. *Cyber Resilience Act*, approvato dal Parlamento europeo a marzo 2024. I principali obiettivi della proposta sono tre: *i)* creare le condizioni per lo sviluppo di prodotti digitali sicuri, garantendo che siano immessi sul mercato *hardware* e *software* con il minor numero di vulnerabilità; *ii)* accrescere la responsabilità degli operatori economici privati, obbligandoli ad assicurare la necessaria attività di supporto e aggiornamento dei prodotti; *iii)* migliorare il livello delle informazioni rese agli utenti in merito alla sicurezza dei beni e dei servizi da loro acquistati. Sul punto, cfr. Chiara 2023: 143 ss.

20 Così, Sales 2018: 632.

21 Cfr. il regolamento UE 2021/887 del 20 maggio 2021.

22 Cfr. la comunicazione congiunta del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, par. 2.1.

network finalizzato ad assicurare un monitoraggio costante, diffuso e in tempo reale delle intrusioni e delle anomalie informatiche nelle reti e nei sistemi di diversi portatori di interesse, anche attraverso il coinvolgimento delle PMI dell'Unione e l'utilizzo di tecnologie avanzate di intelligenza artificiale[23]. Grazie a questa rete, pensata per coordinare i diversi SOC nazionali dislocati su tutto il territorio europeo, vengono potenziate, in particolare, le capacità di rilevamento, di analisi e di condivisione dei dati relativi agli attacchi *cyber* più pericolosi, consentendo ad autorità pubbliche e soggetti privati di segnalare tempestivamente, tramite canali condivisi, minacce potenziali e in corso, prima che queste abbiano causato danni irreparabili su larga scala[24].

Già da questi esempi è possibile ricavare come, nella visione prospettica adottata in sede europea, la gestione del rischio cibernetico richieda la sperimentazione di modelli relazionali diversi rispetto a quelli tradizionali, basati non tanto (o non solo) sulla logica della difesa del "fortino" sperimentata nell'ambito della protezione della sicurezza nazionale[25], quanto su una più strutturata cooperazione tra pubblico e privato.

Tuttavia, se è evidente che la realizzazione del nuovo paradigma non può essere lasciata alla mera adesione volontaria dei soggetti interessati (specie nel breve-medio periodo), risulta necessario stabilire con quali modalità, con quali incentivi ed entro quali limiti la suddetta collaborazione deve avvenire.

In altri termini, la concreta attuazione delle ricordate linee strategiche definite in sede sovranazionale richiede la conclusione di appositi accordi contrattuali tra le parti coinvolte, volti a chiarire, tra gli altri, gli incentivi economici, la ripartizione dei rischi, le condizioni di riservatezza e le clausole di esonero da responsabilità per le imprese del settore[26].

23 Cfr. la comunicazione congiunta del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, par. 1.2.

24 Lo sfruttamento di questo *network* pubblico-privato permetterà di creare quello che viene definito in termini di "scudo europeo di sicurezza informatica" dalla recente proposta di regolamento UE del 18 aprile 2023, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza e di preparazione e risposta agli stessi, COM (2023) 209 final, c.d. *Cyber Solidarity Act*.

25 Cfr. Ursi 2022: 18 ss., il quale osserva che, nei Paesi a democrazia liberale, è il settore privato che detiene la stragrande maggioranza delle reti e delle infrastrutture digitali; in tal senso, gli obblighi introdotti dal nostro legislatore nei confronti dei soggetti ricompresi all'interno del Perimetro nazionale costituirebbero una moderna espressione del dovere di difesa della patria di cui all'art. 52, comma 1, Cost.

26 Sull'importanza dei suddetti accordi contrattuali, cfr. Bossong, Wagner 2017: 284: "*In the area of cybersecurity, other forms of risks and responsibilities beyond timely construction or reliable service provision have to be considered. Governments are also increasingly able to exert pressure to obtain 'voluntary' cooperation from business […]. But when dealing with new or advanced cyber threats, public actors often enter these partnerships as the weaker partner, reliant on specialised IT companies to define the level of vulnerability and appropriate countermeasures*", nonchè Pupillo 2018: 3, secondo il quale "*it is thus clear that new conceptual approaches to cybersecurity are required to make the behaviour of all players in this market more incentive-compatible*"; Taddeo 2019: 351.

Al riguardo occorre rilevare come l'Agenzia dell'Unione europea per la cybersicurezza (*European Union Agency for Network and Information Security*, di seguito ENISA) abbia stimolato più volte gli Stati membri ad agire in questa direzione, identificando, segnatamente, quattro principali paradigmi già presenti in Europa[27]: *i*) l'*Institutional PPP*, finalizzato ad assicurare la protezione di istituzioni e infrastrutture critiche attraverso una cooperazione di lungo periodo tra gli interessati, che si esplica, ad esempio, nello svolgimento di attività di supporto operativo, di analisi dei dati, di elaborazione di buone pratiche, di controllo degli *standard* di sicurezza e di altri servizi[28]; *ii*) il *Goal-oriented PPP*, volto a promuovere la cultura della sicurezza informatica negli Stati membri attraverso la costituzione di centri e di gruppi di scambio di conoscenze e di soluzioni pratiche su specifici argomenti[29]; *iii*) il *Service outsourcing PPP*, utile a rappresentare alle autorità pubbliche competenti le problematiche *cyber* più sentite all'interno di uno specifico contesto imprenditoriale ed a suggerire, di conseguenza, gli opportuni atti normativi e di indirizzo da adottare per risolverle[30]; *iv*) l'*Hybrid PPP*, che costituisce una combinazione del primo e del terzo modello, spesso utilizzato per affidare a qualificati enti privati funzioni e compiti che le stesse istituzioni nazionali non sono in grado di esercitare, come quelli inerenti alle attività di segnalazione e di risposta in caso di attacchi cibernetici[31].

La scelta del modello di partenariato da implementare viene lasciata, invero, ai singoli Stati membri, dal momento che "*there is no universal, simple solution that applies to all the nations for creating and developing PPP. It is rather a national issue, connected with the culture and the way how the whole political and economic system works*"[32].

Dalle richiamate proposte di partenariato è possibile ricavare, a ben vedere, gli ulteriori, rilevanti benefici derivanti dall'instaurazione di una duratura interlocuzione tra autorità pubbliche e mondo imprenditoriale, che non si apprezzano solo con riferimento allo scambio di conoscenze specialistiche e di soluzioni operative[33], ma anche in sede di elaborazione e di aggiornamento delle politiche, delle

27 Cfr. ENISA, *Public Private Partnerships (PPP). Cooperative models*, novembre 2017, par. 3 ss., reperibile in www.enisa.europa.eu.

28 Si tratta del modello diffuso in Estonia e Polonia.

29 Si tratta del modello presente in Spagna, Regno Unito, Lussemburgo, Olanda, Austria, Slovacchia.

30 Si tratta del modello che si trova in Germania e Austria.

31 Modello presente, ad esempio, in Repubblica Ceca.

32 Cfr. ENISA, *Public Private Partnerships (PPP)*, par. 3.

33 Un contributo che non va, tuttavia, sminuito, ma che risulta essere, in ogni caso, prezioso nel contesto in esame, caratterizzato da evidenti asimmetrie informative. Infatti, se, da un lato, la capillarità delle minacce *cyber* e la complessità della tecnologia in commercio rendono le imprese del settore i soggetti più qualificati a comprendere le tattiche d'attacco degli *hackers*, a individuare le principali vulnerabilità nascoste nei *software* e a suggerire alle autorità competenti le contromisure più opportune; dall'altro, la realizzazione di un circuito di sorveglianza e di allerta distribuito (c.d. *distributed surveillance*), che si basa (anche) sulla continua attività di vigilanza svolta dagli operatori economici, può ridurre notevolmente le inefficienze e i costi amministrativi sopportati dagli Stati membri per la tutela della sicurezza cibernetica nazionale. Al riguardo, cfr. Clarke, Knake 2010: 162.

linee guida, dei protocolli e degli *standard* di sicurezza[34], specie nell'ambito della protezione delle infrastrutture e dei servizi considerati "critici", gestiti nella maggior parte dei casi da soggetti privati.

In particolare, l'intervento di questi ultimi nel processo di determinazione delle politiche e delle misure vincolanti per tutti gli *stakeholders* offrirebbe certamente alle autorità competenti un valido supporto tecnico[35]; tale forma di collaborazione consentirebbe, inoltre, di evitare il rischio di perseguire ambiziosi obiettivi di resilienza attraverso l'introduzione di oneri e requisiti inidonei o eccessivi, non compatibili con il principio di proporzionalità e con la prospettiva liberale da preservare in materia[36].

Come è evidente, infatti, aziende ed enti differenti affrontano minacce, vulnerabilità e conseguenze diverse; pertanto, un'effettiva inclusione di tali soggetti nelle sedi decisionali e consultive non potrebbe che favorire la definizione di strumenti parametrati al concreto livello di rischio informatico, adeguati ai particolari contesti in cui operano le imprese e aggiornati rispetto alle innovazioni tecnologiche sopravvenute.

In altri termini, la promozione di nuove forme di cooperazione tra attori pubblici e privati nel settore in esame consentirebbe non solo una maggiore condivisione di informazioni, abilità e buone pratiche, ma anche un'auspicabile partecipazione "dal basso" al processo regolatorio, limitando il tradizionale approccio "*command and control*" per favorire forme di "*enforced self-regulation*"[37].

3. Prove di convergenza nella recente strategia nazionale in materia di cybersicurezza

L'analisi delle recenti indicazioni formulate a livello europeo consente adesso di svolgere alcune considerazioni in merito alle caratteristiche dell'attuale architettura italiana in materia di cybersicurezza.

Al riguardo è possibile rilevare che, al pari dell'originario assetto istituzionale, anche l'ecosistema nazionale ridefinito negli ultimi anni continua a caratterizzarsi, in gran parte, per un chiaro *deficit* di partecipazione degli operatori economici[38]. Una conclusione che trova fondamento nella circostanza per la quale il principale coinvolgimento del settore privato finora sperimentato ha riguardato la fase di pro-

34 Sul punto, cfr. anche Farrand, Carrapico 2018: 197 ss.

35 Cappelletti, Martino 2021: spec. 7 ss.

36 Raffiotta 2022: 13-14, il quale contrappone, all'approccio, per certi versi, "dirigista" del legislatore europeo, il modello liberale adottato dagli Stati Uniti d'America. Secondo l'A., infatti, il paradigma americano, che opera a livello federale attraverso la *Cybersecurity and Infrastructure Security Agency* (CISA), si caratterizza per "*a voluntary approach, within which there is a synergy between a 'light government touch' and a strong empowerment of private entities, including – above all – Big Techs corporations*".

37 Il punto è evidenziato, in particolare, dalla numerosa letteratura internazionale in argomento. Al riguardo, si vedano, quantomeno, Sales 2013: 1554 ss.; Tropina 2015: 9 ss.; Rosenzweig 2012.

38 Su questi profili, cfr. anche Previti 2022: 81 ss.

gettazione e di sviluppo di tecnologie e infrastrutture digitali e non anche, come invece sarebbe stato auspicabile[39], l'implementazione di forme di co-regolamentazione, specie con riferimento al processo di definizione delle regole tecniche e dei requisiti minimi di sicurezza.

Si tratta di una scelta legislativa che suscita, a ben vedere, numerose perplessità, anche in considerazione della nota dipendenza delle nostre pubbliche amministrazioni dalle capacità e dalle esperienze in ambito tecnologico-informatico possedute dalle imprese del settore, che ha rappresentato, e rappresenta ancora, una delle principali cause dei ritardi registrati dal nostro Paese nel complessivo processo di transizione digitale[40].

Le criticità evidenziate conducono ad accogliere con particolare favore le interessanti proposte contenute nella strategia italiana sulla cybersicurezza 2022-2026 – e nel relativo piano di implementazione, che contiene, nel complesso, 82 misure specifiche per le tre macro componenti delineate dalla strategia (Protezione, Risposta, Sviluppo) – adottata nel maggio 2022, quale documento programmatico di primaria rilevanza per la definizione delle priorità di intervento e delle principali sfide da affrontare nel prossimo quinquennio[41].

Oltre che per i necessari interventi nella componente "Sviluppo"[42], i documenti in esame meritano di essere apprezzati per l'introduzione di alcuni importanti assestamenti finalizzati a sfruttare le risorse conoscitive e operative degli operatori privati nell'ecosistema nazionale *cyber*. E ciò sia in relazione agli obiettivi della componente "Protezione" che in relazione agli obiettivi della componente "Risposta"[43].

Nello specifico, con riferimento al primo obiettivo, la strategia mira a potenziare il sistema di certificazione, che fa capo al Centro di Valutazione e Certificazione Nazionale (CVCN) istituito presso l'ACN e, negli ambiti di competenza, ai Centri di Valutazione del Ministero dell'Interno e della Difesa. A tal fine, viene prevista l'introduzione di una rete dei laboratori accreditati di prova (c.d. LAP), quali soggetti, pubblici e privati, chiamati a supportare le procedure di certificazione della qualità degli *asset* tecnologici utilizzati dai soggetti inclusi nel PSNC e a individuare le relative vulnerabilità[44].

39 Lauro 2021: 537 ss.; Cusenza 2023: 130 ss.

40 In merito si rinvia, *ex multis*, a Sgueo 2022.

41 Per un'analisi della nuova strategia nazionale, cfr. Matassa 2022: 625 ss.

42 Al riguardo è interessante notare che, tra le misure indicate nel citato piano di implementazione, reperibile al sito www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza, vengono ricomprese la realizzazione di un "parco nazionale della cybersicurezza" (misura 49), finalizzato allo svolgimento di attività di ricerca e sviluppo nell'ambito della *cybersecurity* e delle tecnologie digitali tramite il coinvolgimento di competenze e risorse provenienti dal settore pubblico, imprenditoriale e accademico, nonché l'implementazione di un "piano per l'industria *cyber* nazionale" (misura 51), volto a sostenere imprese e *startup* per la progettazione e la realizzazione di prodotti e servizi ad alta affidabilità.

43 Nel complesso, gli operatori privati risultano coinvolti nella realizzazione di ben 27 misure.

44 Con riferimento alla funzione di certificazione in ambito *cyber*, cfr. Bruno 2020: 11 ss.;

Allo stesso tempo, con riferimento al secondo obiettivo, viene espressamente sottolineata la necessità di sfruttare le capacità nazionali di identificazione e di risposta in caso di attacchi *cyber*, prevedendo due peculiari forme di collaborazione tra gli operatori economici e l'ACN.

La prima, di natura strutturale, riguarda l'istituzione di una rete di centri settoriali di analisi e di condivisione di informazioni rilevanti (*Information Sharing and Analysis Center*, c.d. ISAC), chiamata a supportare gli uffici dell'ACN nel predisporre e nel diffondere buone pratiche, linee guida, avvisi di sicurezza e raccomandazioni all'interno del Paese.

La seconda, di natura occasionale, contempla il coinvolgimento diretto di aziende qualificate in materia di *incident response,* a supporto delle funzioni istituzionali dello CSIRT Italia, nel caso in cui dovesse verificarsi 'una moltitudine di incidenti *cyber* di natura sistemica'.

Attraverso tali misure, l'Italia mostra dunque di voler utilizzare non solo adeguate strategie di resilienza, ma anche efficaci tattiche di difesa attiva (*active difense*), con l'intento di sviluppare, avvalendosi di una molteplicità di sorgenti di dati rilevanti e di attori responsabili, forme partecipate e tempestive di gestione delle crisi e di contrattacco[45]: una circostanza che assume contorni affatto singolari, come è evidente, nel caso in cui l'attacco informatico abbia assunto una rilevanza tale da mettere in pericolo la stessa sicurezza nazionale[46].

4. Implicazioni sistematiche e nuovi interrogativi

Le considerazioni sopra effettuate consentono adesso di trarre le implicazioni sistematiche derivanti dal progressivo processo di avvicinamento delle linee strategiche italiane in materia di cybersicurezza alle direttrici fissate negli ultimi anni a livello sovranazionale.

Da quanto si è detto è emerso come gli operatori del settore possano occupare un vero e proprio ruolo da co-protagonista all'interno del sistema multilivello di tutela della sicurezza cibernetica.

Volendo riassumere di seguito gli ambiti di effettiva implementazione della menzionata cooperazione pubblico-privato, è possibile notare come le funzioni e i processi coinvolti da tale operazione riguardino, quantomeno: *i)* la progettazione, la produzione e la fornitura di beni e servizi *online*; *ii)* lo studio, l'analisi e la conoscenza delle vulnerabilità e delle minacce informatiche; *iii)* la condivisione e lo scambio di informazioni, esperienze, buone pratiche e soluzioni operative; *iv)* la certificazione e la verifica del possesso di determinati *standard* qualitativi; *v)* il monitoraggio, il rilevamento e la gestione di crisi cibernetiche; *vi)* la regolazione normativa e tecnica, inclusi l'elaborazione e l'aggiornamento di protocolli, linee

Serini 2023: 41 ss.

45 Su punto, cfr. Gori 2019: 17 ss.

46 Sulle caratteristiche specifiche della c.d. *cyber defence*, cfr. Ursi 2023: 13 ss.

guida, codici di condotta, misure e requisiti minimi di sicurezza; *vii)* lo sfruttamento di competenze tecniche specialistiche e la formazione e l'aggiornamento del personale delle pubbliche amministrazioni.

Si tratta, con evidenza, di un coinvolgimento potenzialmente molto esteso, che abbraccia ambiti particolarmente ampi e importanti, come quello, più tradizionale e sperimentato, dello sviluppo tecnologico, quello, più delicato e operativo, della gestione e della difesa, nonché quello, più strategico e complesso, della prevenzione e della resilienza.

Orbene, se quella appena delineata rappresenta la direzione verso la quale le politiche europee e nazionali in materia di cybersicurezza stanno lentamente convergendo, l'attuale processo di assestamento dell'architettura italiana pare poter costituire l'occasione per affrontare alcuni rilevanti interrogativi di fondo.

Il primo interrogativo riguarda la possibilità di continuare a gestire le peculiari problematiche connesse alla salvaguardia della pubblica sicurezza nel cyberspazio tramite moduli operativi e organizzativi ispirati, seppur in maniera ridotta rispetto alla disciplina previgente, a logiche e principi tipici del settore della sicurezza nazionale[47].

Al contrario, anche alla luce delle richiamate indicazioni di matrice europea, sembra ragionevole sostenere come nel contesto in esame il raggiungimento di un soddisfacente livello di resilienza e difesa richieda l'adozione di schemi e misure tipici di un settore aperto e multipartecipato, che assume sempre più le sembianze di un vero e proprio mercato di beni e servizi, rispetto al quale è necessario assicurare certezza giuridica e preservare la fiducia degli utilizzatori e degli utenti[48].

A tale considerazione si aggiunga che l'integrazione di attori privati nell'articolato sistema di sicurezza cibernetica rappresenta, nel nostro ordinamento, più un'esigenza strutturale, specie nel breve-medio periodo, che una libera presa di posizione; e ciò in considerazione della nota condizione di debolezza tecnologica e informatica in cui versa la gran parte delle pubbliche amministrazioni italiane e, di conseguenza, del frequente ricorso allo strumento dell'esternalizzazione.

Il secondo interrogativo, strettamente connesso al primo, attiene, invece, al possibile ripensamento del ruolo finora attribuito allo Stato all'interno del nuovo contesto istituzionale[49].

47 Si pensi, in tal senso, alla perdurante centralità delle attribuzioni affidate al Presidente del Consiglio dei ministri dal d.l. n. 82/2021, alla segretezza dell'elenco dei soggetti inseriti all'interno del PSNC ai sensi del d.l. n. 105/2019, all'operazione di centralizzazione delle funzioni istituzionali realizzata con l'istituzione dell'ACN, continuata, invero, anche dalle recenti modifiche introdotte dalla citata l. n. 90/2024.

48 Si pensi, in tal senso, alle politiche di *risk management* e di *risk regulation* mutuate dall'ambito privatistico, così come alla normativa multilivello in materia di certificazioni. Al riguardo, cfr. anche Serini 2023: 46, secondo il quale la stessa disciplina europea suggerisce che l'infrastruttura logica e materiale del cyberspazio può essere interpretata come "un agglomerato di prodotti, processi e servizi che attengono alle tecnologie dell'informazione e della comunicazione che circolano nel mercato globale".

49 In materia, si vedano anche le recenti e interessanti considerazioni di Casini 2020; Torchia 2023.

Al riguardo, se è, da un lato, comprensibile una certa difficoltà nel pronunciare quella "confessione di fallimento"[50] nel gestire e assicurare, con autonomia di decisioni e risorse, la sicurezza pubblica nel cyberspazio, occorre domandarsi, dall'altro, quale compito possa essere riservato alle autorità nazionali laddove le caratteristiche del fenomeno implicano, come si è visto, l'attuazione di politiche e di meccanismi di redistribuzione e condivisione del rischio tra tutti i soggetti coinvolti nel processo di sicurezza (dalla progettazione del dispositivo tecnologico fino alla difesa in caso di attacchi).

Si tratta, a ben vedere, di un interrogativo di particolare complessità, in relazione al quale, probabilmente, non è dato rinvenire una soluzione soddisfacente *a priori*, potendosi unicamente escludere il ritorno a un ambiente "incontaminato", caratterizzato dall'assenza di regole e vincoli giuridici da parte degli Stati[51].

In prima battuta, si sarebbe tentati di rispondere al quesito invocando l'attuazione del modello, dominante in Italia nell'ultimo trentennio, dello "Stato regolatore", che si riserva un ruolo di garante del funzionamento dei settori economici e di vigilanza sulla corretta applicazione delle regole (in questo caso, di sicurezza) dettate per i singoli mercati, limitando, se non necessario, il proprio intervento proattivo nei processi produttivi[52].

Eppure, una delle più celebri elaborazioni dottrinali che ha indagato il rapporto tra potere statale e sviluppo tecnologico non esita ad assegnare allo Stato il ruolo di protagonista dell'innovazione (c.d. "Stato innovatore"), dal momento che quest'ultimo rappresenterebbe l'unico soggetto in grado di assumersi, per primo, il rischio di impresa (*i.e.* l'incertezza del successo) e di investire ingenti risorse a lungo termine, nell'ottica del perseguimento di importanti benefici per la collettività. Secondo tale teoria, infatti, è l'autorità nazionale a dover intervenire, in prima persona, per coinvolgere e stimolare le imprese interessate a sviluppare nuova tecnologia, stabilendo chiaramente, in primo luogo, gli obiettivi strategici da raggiungere e socializzando, poi, i costi e i ricavi dell'operazione promossa[53].

Applicando la menzionata impostazione al settore della cybersicurezza, parte della dottrina ha così sostenuto che l'intervento statale, lungi dall'assumere il ruolo di arbitro e di mero regolatore delle dinamiche di mercato, dovrebbe tendere a implementare forme e meccanismi di c.d. "collaborazione orientata", ossia indirizzata al perseguimento degli indirizzi di lungo periodo predefiniti dalle istituzioni pubbliche[54].

50 Monti 2020: 75. Sulle inevitabili difficoltà che i pubblici poteri incontrano nel regolare le relazioni e i rapporti umani che hanno luogo nello spazio virtuale, si vedano, da ultimo, Mannoni, Stazi 2021; Betzu 2022.

51 Cfr. Pollicino 2023: 415, il quale sottolinea, al contrario, la recente tendenza degli Stati a "iper-regolare" il cyberspazio.

52 Cfr. La Spina, Majone 2000; D'Alberti, Tesauro 2000; Police 2007.

53 In tal senso, Mazzucato 2020 [2013]: spec. 15 ss.

54 Cfr. Rossa 2023: spec. 207 ss., secondo il quale, per assicurare la cybersicurezza delle reti e delle infrastrutture digitali utilizzate a fini pubblici, uno degli strumenti più adeguati sarebbe rappresentato dagli appalti innovativi (e, in particolare, dal partenariato per l'innovazione), che consentirebbe alle stazioni appaltanti e agli operatori privati fornitori di tecnologia di co-

In tal senso, spetterebbe allo Stato esercitare un'importante funzione pianificatoria, che si traduce nella fissazione delle priorità di intervento, degli obiettivi di interesse generale, degli strumenti, dell'orizzonte temporale e delle risorse economiche necessari, evitando così di venire "catturato" dagli interessi particolari di cui è portatore il produttore o il fornitore del bene o del servizio tecnologico.

In ogni caso, a prescindere dalle scelte di politica economica e finanziaria compiute dall'ordinamento[55], rimane ferma la necessità di definire, tra i diversi soggetti coinvolti nel sistema di sicurezza cibernetica, un equilibrato assetto di interessi, che assegna agli attori istituzionali l'individuazione delle linee strategiche e che, al contempo, ingloba gli operatori privati, secondo modalità variegate, nel processo di attuazione.

Questo passaggio appare, in definitiva, l'unica alternativa possibile per raggiungere, nel lungo periodo, una stabile e consolidata "sovranità tecnologica" a livello nazionale ed europeo, che non dipenderà solamente dall'ammontare e dalla destinazione degli investimenti finanziari dei prossimi anni, ma anche dalla sapiente inclusione delle risorse e delle competenze esistenti nell'attuale tessuto sociale.

Bibliografia

Amato Mangiameli A.C., Saraceni G. (a cura di) 2019, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino: Giappichelli.

Baroni M. 2022, "Intelligenza artificiale e cybersicurezza in una prospettiva costituzionale", in G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (a cura di), *AI Anthology*, Bologna: Il Mulino: 373 ss.

Bassanini F., Napolitano G., Torchia L. 2021, *Lo Stato innovatore. Come cambia l'intervento pubblico nell'economia*, Bologna: Il Mulino: spec. 231 ss.

Bassini M. 2021, "Cybersecurity", in M.T. Paracampo (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino: Giappichelli: 319 ss.

Betzu M. 2022, *I baroni del digitale*, Napoli: Editoriale scientifica.

Bossong R., Wagner B. 2017, "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union", in *Crime, Law and Social Change*, 67 (3): 284.

Brighi R., Chiara P.G. 2021, "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea", in *Federalismi.it*, (21): 20 ss.

Bruno B. 2020, "Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *Federalismi.it*, (14): 11 ss.

creare il bene o il servizio necessario, dotato di caratteristiche *cybersafe by design*, evitando al contempo il verificarsi delle conseguenze negative legate alla produzione del c.d. effetto *lock-in*.

55 Si tratta di politiche che sono spesso legate alle contingenze temporali e alle diverse caratteristiche (storiche, politiche, culturali, ecc.) dei singoli Paesi. Per una disamina della recente evoluzione delle politiche italiane di promozione dell'iniziativa economica privata, anche con riferimento al settore dell'innovazione tecnologica, cfr. Bassanini, Napolitano, Torchia 2021: spec. 231 ss.

Cappelletti F., Martino L. 2021, "Achieving robust European cybersecurity through public-private partnerships: approaches and developments", in *Elf discussion paper*, (4): spec. 7 ss.
Carotti B. 2020, "Sicurezza cibernetica e Stato nazione", in *Giornale di diritto amministrativo*, (5): 629 ss.
Casini L. 2020, *Lo Stato nell'era di Google. Frontiere e sfide globali*, Milano: Mondadori.
Chiara P.G. 2023, "Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali", in *Rivista italiana di informatica e diritto*, (1): 143 ss.
Clarke A., Knake R.K. 2010, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins Publishers: 162.
Contaldo A., Mula D. (a cura di) 2020, *Cybersecurity Law*, Pisa: Pacini: 57 ss.
Cusenza G. 2023, "I poteri dell'Agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico", in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 130 ss.
D'Alberti M., Tesauro G. (a cura di) 2000, *Regolazione e concorrenza*, Bologna: Il Mulino.
Farrand B., Carrapico H. 2018, "Blurring public and private: cybersecurity in the age of regulatory capitalism", in O. Bures, H. Carrapico (editors), *Security Privatization. How non-security-related Private Businesses Shape Security Governance*, Cham: Springer: 197 ss.
Forgione I. 2022, "Il ruolo strategico dell'Agenzia nazionale per la cybersicurezza nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", in *Diritto amministrativo*, (4): 1113 ss.
Franchini M. 2010, "Il sistema nazionale delle informazioni per la sicurezza e l'autorità delegata", in *Giornale di diritto amministrativo*, (4): 431 ss.
Gori U. 2019, "Nuovi approcci alla sicurezza cibernetica: la diplomazia preventiva come strumento di difesa attiva", in U. Gori (a cura di), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Milano: Franco Angeli: 17 ss.
Kohler C. 2020, "The EU Cybersecurity Act and European standard: an introduction to the role of European standardization", in *International Cybersecurity Law Review*, (1): 7 ss.
La Spina A., Majone G. 2000, *Lo Stato regolatore*, Bologna: Il Mulino.
Lauro A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *La Rivista Gruppo di Pisa*, (3): spec. 537.
Mannoni S., Stazi G. 2021, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli: Editoriale scientifica.
Matassa M. 2022, "Una strategia nazionale a difesa del cyberspazio", in *P.A. Persona e amministrazione*, (2): 625 ss.
Mazzucato M. 2020 [2013], *Lo Stato Innovatore. Sfatare il mito del pubblico contro il privato,* trad. it. a cura di F. Galimberti, Roma-Bari: Laterza: spec. 15 ss.
Mele S. 2020, "Il Perimento di sicurezza nazionale cibernetica e il nuovo 'golden power'", in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano: Giuffrè: 186 ss.
Montessoro P.L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Istituzioni del Federalismo*, (3): 783 ss.
Monti A. 2020, "Internet e ordine pubblico", in G. Cassano, S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano: Giuffrè: 75.

Paganini P. 2022, "Cybercrime-as-a-Service: EU Perspectives", in L. Martino, N. Gamal (a cura di), *European Cybersecurity in Context. A Policy-Oriented Comparative Analysis*, Elf study: 67 ss.
Parona L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale di diritto amministrativo*, (6): 713 ss.
Police A. 2007, *Tutela della concorrenza e pubblici poteri*, Torino: Giappichelli.
Pollicino O. 2023, voce "Potere digitale", in *Enciclopedia del diritto. Potere e Costituzione*, V, Milano: Giuffrè: 415.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it*, (25): 81 ss.
Pupillo L. 2018, "EU Cybersecurity and the Paradox of Progress", in *CEPS policy insights*, (6): 3.
Raffiotta E.C. 2022, "Cybersecurity regulation in the European Union and the issues of Constitutional Law", in *Rivista AIC*, (4): 13-14.
Renzi A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giornale di diritto amministrativo*, (4): 538 ss.
Rodotà S. 2014, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari: Laterza: 3.
Rosenzweig P. 2012, *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World*, Westport: Praeger Press.
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica: spec. 207 ss.
Sales N.A. 2013, "Regulating Cyber-Security", in *Northwestern University Law Review,* 107 (4): 1554 ss.
Sales N.A. 2018, "Privatizing Cybersecurity", in *UCLA Law Review,* 65 (3): 632.
Serini F. 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", in *Federalismi.it*, (12): 241 ss.
Serini F. 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*, (2): 41 ss.
Sgueo G. 2022, *Il divario. I servizi pubblici digitali tra aspettative e realtà*, Milano: Egea.
Taddeo M. 2019, "Is Cybersecurity a Public Good?", in *Minds & Machines*, (29): 351-352.
Torchia L. 2023, *Lo Stato digitale. Una introduzione*, Bologna: Il Mulino.
Tropina T. 2015, "Public-private collaboration: Cybercrime, cybersecurity and nationals security", in T. Tropina, C. Callanan (eds.), *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Cham: Springer: 9 ss.
Ursi R. 2022, "La difesa: tradizione e innovazione", in *Diritto Costituzionale*, (1): 18 ss.
Ursi R. 2023, "La sicurezza cibernetica come funzione pubblica", in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 13 ss.
Ziccardi G. 2019, "La cybersecurity nel quadro tecnologico (e politico) attuale", in G. Ziccardi, P. Perri (a cura di), *Tecnologia e diritto*, III, Milano: Giuffrè: 210.

Lorenzo Ricci

Il Comitato interistituzionale per la cibersicurezza e la direzione strategica del CERT-EU: verso una 'regolazione strategica' della cibersicurezza?

Abstract: L'articolo si apre con l'esame del Comitato interistituzionale per la sicurezza informatica (IICB). Il Regolamento (UE) 2023/2841, oltre ad assegnare maggiori compiti e un ruolo più ampio al CERT-EU, attribuisce a questo organo il duplice compito di monitorare e sostenere l'attuazione del regolamento citato, da parte degli attori dell'UE, nonché di supervisionare l'attuazione delle priorità e degli obiettivi generali del CERT-EU, con la possibilità di fornire una direzione strategica a questa entità. Si tratta, quindi, di riflettere sull'organizzazione e sulle funzioni attribuite a questo board, nel tentativo di evidenziare il ruolo che si intende attribuirgli e, soprattutto, i poteri normativi che lo caratterizzano, nella direzione di configurare un modello omogeneo ed efficace di regolamentazione della cybersecurity.

Keywords: ICBB; CERT-EU; Coordinamento; Direzione strategica; Regolazione strategica.

1. Premessa

Il regolamento (UE) 2023/2841 ha istituito il Comitato interistituzionale per la cibersicurezza (IICB), al duplice scopo di controllare e sostenere l'attuazione del presente regolamento da parte dei soggetti dell'UE, nonché di vigilare in relazione alla realizzazione delle priorità e degli obiettivi generali del CERT-EU, con la possibilità di imprimere a tale centro una direzione di tipo strategico. Sotto questo profilo, il regolamento in questione ha inoltre attribuito maggiori compiti nonché un più ampio ruolo al CERT-EU.

Pertanto, si tenterà anzitutto di riflettere sull'organizzazione e sulle funzioni che sono attribuite a questo Comitato[1], per cercare di chiarire il ruolo che si è inteso attribuirgli e, in special modo, i poteri di regolazione che lo caratterizzano, nella direzione di configurare un sistema omogeneo ed efficace di cibersicurezza a livello europeo.

1 Più in generale, sul ruolo dei Comitati a livello europeo, per tutti, cfr. Savino 2005.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760164

Nello specifico, dopo aver effettuato la ricostruzione dell'assetto organizzativo, si pone come necessario metterne in luce le relative relazioni intersoggettive, sia per quanto attiene a quelle di tipo organizzativo che a quelle concernenti i profili funzionali; invero, tale Comitato è destinato ad intrattenere 'intensi' rapporti con il CERT-EU. Inoltre, vengono in rilievo anche le relazioni con l'ENISA[2], nella direzione di un assetto destinato ad essere caratterizzato da una rilevante presenza di questi tre 'soggetti'.

Infine, suscita notevole interesse esaminare gli strumenti e le modalità attraverso le quali il Comitato è destinato ad operare. È quindi opportuno porre l'accento sul potere riconosciuto a tale 'organismo' circa la facoltà di adottare una strategia, su base pluriennale, al fine di innalzare il livello di cibersicurezza nei soggetti appartenenti all'UE. Da questo punto di vista – come si vedrà meglio più avanti – il Comitato valuta periodicamente tale strategia e, in ogni caso, è comunque tenuto a farlo ogni cinque anni, potendo altresì – ove lo dovesse reputare necessario – procedere ad una sua modifica.

Si è dinanzi ad un potere che assume particolare significato in ragione delle sue potenzialità circa la (possibile) configurazione di una regolazione strategica del CERT-EU e, di conseguenza, della cibersicurezza nel suo complesso.

La domanda di ricerca, invero, ha come obiettivo, in ultima analisi, proprio quello di tentare di riflettere attorno all'interrogativo concernente la possibilità per cui, attraverso il Comitato e i poteri di direzione nei confronti del CERT-EU che gli sono attribuiti, sulla base anche della strategia europea in materia, si vada verso una regolazione strategica della cibersicurezza, anche per il tramite di un maggior coordinamento (e, dunque, di una più efficace cooperazione) fra i vari soggetti che, a diverso titolo, sono chiamati alla regolazione di tale fenomeno[3].

L'ipotesi di partenza, infatti, è che la cibersicurezza richieda una regolazione pubblica[4] in grado di essere flessibile per meglio adattarsi ai repentini mutamenti che interessano il mondo delle tecnologie e, quindi, ai relativi attacchi informatici. La giustificazione ultima di questo modello di regolazione non può che rinvenirsi nella protezione dei diritti che da tali attacchi rischiano di essere lesi, quegli stessi diritti che, in ragione del carattere personalista[5] tanto dell'ordinamento europeo quanto delle costituzioni (di quasi tutti) i paesi che ne fanno parte, a partire da quella italiana, devono inevitabilmente rappresentare il punto di partenza di ogni riflessione in ambito giuridico.

2 Più in generale, sul ruolo delle Agenzie nell'organizzazione delle amministrazioni europee (e la loro articolazione in forma 'reticolare') cfr., per tutti, Chiti, 2002; Chiti 2009.

3 Sul punto, di recente, cfr. Camisa, Simoncini 2024.

4 In proposito, di recente, Lalli 2024. Nella prospettiva della co-regolazione, che si può considerare come una forma di regolazione intermedia tra quella privata (autoregolazione) e quella pubblica (eteroregolazione) e che sembra essere il modello regolatorio su cui si fondano sia il *Digital Markets Act* che il *Digital Services Act*, cfr. Simoncini 2022. Sul punto cfr. anche Iannuzzi 2023.

5 Cfr. Caterina 2023.

2. Composizione, funzionamento e ruolo del IICB

Per quanto attiene alla composizione del IICB, senza elencare tutte le quindici istituzioni europee che ne fanno parte[6], il regolamento prevede che, oltre alla totalità degli organi dell'UE[7], per quanto concerne i soggetti più direttamente interessati alla cibersicurezza, vi sia un rappresentante del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca, uno dell'ENISA e, infine, un rappresentante del Garante europeo della protezione dei dati (GEPD). Inoltre, sono previsti tre rappresentanti designati dalla rete delle agenzie dell'Unione (EUAN) su proposta del suo comitato consultivo TIC per difendere gli interessi degli organi e degli organismi dell'Unione che gestiscono il proprio ambiente TIC, ovviamente diversi dai soggetti espressamente elencati che hanno già, appunto, un proprio rappresentante[8]. Di conseguenza, il Comitato può contare sui quindici rappresentanti di cui sopra, ai quali si aggiungono i tre designati dall'EUAN, per un totale di diciotto membri.

Si stabilisce che ciascun componente possa farsi assistere da un supplente e che, in aggiunta ai diciotto membri, le istituzioni europee – oltre al proprio rappresentante – possano vedere invitati, da parte del presidente del Comitato, ulteriori rappresentanti allo scopo di assistere alle riunioni dello stesso Comitato, senza tuttavia che sia loro riconosciuto il diritto di voto[9]. Il Comitato è tenuto ad adottare un proprio regolamento interno[10] e a designare tra i suoi membri – conformemente allo stesso regolamento – un presidente, il cui mandato ha durata triennale[11]. Il Comitato è, inoltre, chiamato a riunirsi almeno tre volte l'anno, riunione che avviene o su iniziativa del suo presidente, o su richiesta del CERT-EU o, infine, a seguito della richiesta di uno dei componenti[12].

Per quanto riguarda, invece, il profilo relativo al diritto di voto, è previsto che ciascun membro sia titolare di un voto e che le decisioni siano adottate a maggioranza semplice, con l'eccezione di quei casi in presenza dei quali il regolamento disponga diversamente.

interessante sottolineare che il presidente non è titolare, generalmente, del diritto di voto, diritto che, tuttavia, sorge in capo ad egli allorché si presenti una situazione di parità (di voti). In questo modo, si riconosce al presidente la facoltà di esprimere quello che è, a tutti gli effetti, il voto decisivo per uscire dall'eventuale stato di impasse ed arrivare così ad una scelta[13].

6 Cfr. art. 10, par. 3, lett. *a*).

7 E cioè: Parlamento europeo, Consiglio europeo, Consiglio dell'Unione europea (o Consiglio, se si preferisce), Commissione europea, Corte di Giustizia europea, Corte dei Conti europea e Banca centrale europea.

8 Art. 10, par. 3, lett. *b*).

9 Art. 10, par. 4.

10 Art. 10, par. 6.

11 Art. 10, par. 7.

12 Art. 10, par. 8.

13 Art. 10, par. 9.

In relazione alla procedura deliberativa, si stabilisce che essa si svolga sulla base di una procedura semplificata e che la decisione finale, in assenza di obiezioni da parte di uno dei membri, sia considerata approvata entro il termine fissato dal presidente del Comitato[14].

Con riferimento, poi, ai rappresentanti nominati dall'EUAN, il regolamento stabilisce che essi trasmettano le decisioni assunte in seno al Comitato ai membri dello stesso EUAN e che a ciascuno di loro sia riconosciuta la facoltà di sottoporre ai membri nominati per far parte del Comitato o, addirittura, al presidente stesso di quest'ultimo, qualsiasi tipo di decisione che si ritenga debba essere posta all'attenzione del Comitato[15].

Un potere del Comitato che potrebbe assumere particolare rilievo è quello che consiste nella facoltà, espressamente attribuitagli, di istituire un comitato esecutivo con il compito di farsi assistere, potendo prevedere nei suoi confronti una delega sia di compiti che di poteri[16].

Rispetto invece al resoconto – e quindi al relativo conseguente controllo – dell'attività svolta dal Comitato, il legislatore ha disposto che quest'ultimo, entro l'8 gennaio 2025 e, successivamente, con cadenza annuale, presenti tanto al Parlamento quanto al Consiglio una relazione illustrativa dei progressi compiuti in punto di attuazione del presente regolamento; inoltre, si stabilisce che tale relazione debba precisare la tipologia di cooperazione intrattenuta dal CERT-EU "con i suoi omologhi degli Stati membri in ciascuno Stato membro". La relazione così definita – si legge – "costituisce un contributo alla relazione sullo stato della cibersicurezza nell'Unione adottata a norma dell'articolo 18 della direttiva (UE) 2022/2555"[17].

Esaminata la composizione dell'istituito Comitato, preme soffermare ora l'attenzione sul profilo attinente ai compiti che il legislatore europeo ha inteso attribuirgli. Coerentemente alla previsione del duplice compito – già ricordato – consistente, da un lato, nel controllare e sostenere l'attuazione del presente regolamento da parte dei soggetti dell'UE e, dall'altro, nel vigilare sull'attuazione delle priorità, nonché degli obiettivi di tipo generale da parte del CERT-EU, e imprimere a quest'ultimo una direzione definita espressamente come 'strategica', si prevede – per quello che qui più interessa e, dunque, con particolare riguardo al CERT-EU – anzitutto che esso fornisca orientamenti al direttore del CERT-EU e che, con riferimento al compito di vigilare e sostenere l'attuazione del regolamento, sostenga i soggetti dell'UE nel compito nient'affatto agevole ma, ciò nonostante, fondamentale, in relazione all'opera di rafforzamento del loro livello di cibersicurezza[18], anche, se del caso, mediante la facoltà di richiedere relazioni *ad hoc* ai soggetti dell'UE e

14 Art. 10, par. 11.
15 Art. 10, par. 12.
16 Art. 10, par. 13.
17 Art. 10, par. 14.
18 Sulla qualificazione della 'robustezza dei sistemi informatici' come interesse pubblico, cfr. Brighi, Chiara 2021: 26-27.

allo stesso CERT-EU. Inoltre, il regolamento attribuisce a tale Comitato, previa discussione strategica, il potere di adottare una strategia, su base pluriennale, che abbia quale fine ultimo quello di innalzare il livello di cibersicurezza nei soggetti dell'UE, e ciò – come già anticipato – mediante una valutazione periodica di tale strategia, essendo comunque in ogni caso tenuta ad analizzarla ogni cinque anni, potendo sempre, ove lo dovesse reputare necessario, procedere ad una sua modifica.

Quest'ultimo compito, unitamente ai poteri di direzione strategica di cui il Comitato è titolare, rappresenta un aspetto fondamentale per affrontare il profilo – come si tenterà di spiegare più avanti – relativo all'ipotesi di una regolazione di tipo strategico della cibersicurezza.

Un altro compito rilevante che il legislatore ha attribuito al Comitato è quello concernente il potere di approvare, sulla base di una proposta avanzata dal presidente del CERT-EU, il programma di lavoro annuale di quest'ultimo, controllandone la relativa attuazione. Allo stesso modo, rivestono importanza i poteri di approvazione – sempre sulla base del medesimo meccanismo da ultimo descritto – della pianificazione finanziaria annuale delle entrate e delle spese (comprese quelle in materia di personale), per le attività proprie del CERT-EU, nonché della relazione annuale elaborata dal presidente del CERT-EU avente ad oggetto sia le attività di quest'ultimo che la relativa gestione dei fondi.

Infine, preme evidenziare altri tre poteri che, per quanto non direttamente collegati con il CERT-EU, presentano profili di sicuro interesse ai fini del presente scritto.

Invero, la facoltà riconosciuta al Comitato circa l'istituzione di gruppi di consulenza tecnica con l'obiettivo di farsi assistere nello svolgimento della propria attività, approvando il loro operato, oltre a designarne i relativi presidenti, rappresenta un potere di peculiare importanza poiché consente al Comitato di dotarsi delle necessarie specifiche conoscenze (in punto di cibersicurezza) che sono fondamentali affinché possa svolgere efficacemente i propri compiti. Il secondo potere attiene, invece, alla valutazione dei documenti e delle relazioni presentate dai soggetti dell'UE sulla base di quanto previsto dal presente regolamento come, per esempio, quelle concernenti le c.d. 'valutazioni di maturità' della cibersicurezza. Infine, il Comitato istituisce un piano relativo alla gestione delle crisi informatiche con la duplice finalità di sostenere – anzitutto sotto il profilo operativo – la gestione coordinata degli incidenti più gravi che possono colpire i soggetti dell'UE, da una parte, e, dall'altra, di contribuire al regolare scambio delle informazioni necessarie, avuto particolare riguardo all'impatto nonché all'entità di siffatti incidenti, oltre che ai possibili modi per (quantomeno) attenuarne i relativi effetti.

3. I nuovi compiti del CERT-EU e l'importanza della cooperazione

Il regolamento (UE) 2023/2841, oltre a dettare misure per un livello più elevato di cibersicurezza nei soggetti dell'UE e a prevedere l'istituzione del IICB, amplia i

compiti del CERT-EU[19]. Invero, dopo averne mutato la denominazione[20], si stabiliscono disposizioni precise circa la sua organizzazione nonché il relativo funzionamento e, più in generale, in merito alla sua operatività.

Si afferma anzitutto che la missione del CERT-EU consiste nel contribuire alla sicurezza dell'ambiente TIC (che non sia riservato) di tutti i soggetti dell'UE e ciò avviene fornendo loro un'attività di consulenza in materia di cibersicurezza che si manifesta anche mediante un aiuto rispetto alla prevenzione ed al rilevamento degli incidenti, aiuto che consiste anche ovviamente nell'affrontare (o comunque attenuare) siffatti incidenti. Il CERT-EU, per questi soggetti, secondo il legislatore europeo, deve assumere il ruolo di una piattaforma in grado di scambiare le informazioni sulla cibersicurezza ed assicurare il coordinamento della risposta in caso di incidenti[21].

Per fare ciò il CERT-EU raccoglie, gestisce, analizza e condivide informazioni con i soggetti dell'UE in relazione alle minacce informatiche, le vulnerabilità e gli incidenti che riguardano le infrastrutture TIC. Inoltre, svolge un'azione di coordinamento delle risposte agli incidenti a livello tanto interistituzionale quanto a livello di soggetti dell'UE, e ciò anche attraverso un'attività che sia in grado di fornire e/o coordinare un'assistenza operativa di tipo specialistico[22].

Il legislatore detta poi i compiti del CERT-EU necessari per assistere i soggetti dell'UE[23] nonché le modalità attraverso le quali contribuire all'attuazione del presente regolamento.

Con riferimento ai primi, fra i tanti – per quello che qui più interessa – merita richiamare i servizi CSIRT standard che offre ai soggetti dell'UE mediante un pacchetto di servizi di cibersicurezza che sono espressamente descritti nel proprio catalogo di servizi (c.d. 'servizi base')[24], così come rilevante è il potere di richiamare l'attenzione del IICB rispetto a qualsiasi tipo di problema concernente l'attuazione del presente regolamento e degli indirizzi, delle raccomandazioni e degli inviti a intervenire[25]. Anche la possibilità di una stretta cooperazione con l'ENISA sulla base delle informazioni raccolte di cui sopra[26] costituisce un potere rilevante che va nella direzione, giustappunto, di un maggiore coordinamento nel 'governo'

19 La stessa Commissione europea, attraverso un comunicato, ha affermato che il regolamento (UE) 2023/2841 prevede un mandato ampliato del CERT-EU sul presupposto per cui si tratti di un polo di scambio di informazioni nonché coordinamento della risposta agli incidenti, un organo, cioè, con funzioni consultive istituito a livello centrale e fornitore di servizi.

20 La nuova denominazione, secondo quanto previsto dal punto 19 dei *Considerando*, dovrebbe essere "Servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione"; tuttavia, allo scopo di facilitarne il riconoscimento, sembra destinata a mantenere l'attuale acronimo.

21 Art. 13, par. 1.

22 Art. 13, par. 2.

23 Si tratta di compiti espressamente previsti all'art. 13, par. 3.

24 Art. 13, par. 3, lett. *b*).

25 Art. 13, par. 3, lett. *d*).

26 Art. 13, par. 3, lett. *e*).

della cibersicurezza[27] che, in questo caso, passa attraverso una inevitabile serrata interlocuzione con il soggetto che, a livello europeo, è preordinato a configurare le condizioni per un elevato livello comune di cibersicurezza. Inoltre, il CERT-EU ha il compito fondamentale di coordinare la gestione degli incidenti ritenuti gravi[28].

Per quanto concerne il profilo della cooperazione, si specifica che il CERT-EU può cooperare con le competenti autorità di cibersicurezza all'interno dell'UE (e dei suoi Stati membri) anche negli ambiti relativi: *i*) alla preparazione, al coordinamento (in caso di incidente), allo scambio di informazioni e risposta alle crisi che si sono verificate a livello tecnico rispetto a casi che hanno coinvolto soggetti dell'UE; *ii*) alla cooperazione operativa per quanto concerne la rete CSIRT (compresa l'assistenza reciproca); *iii*) all'*intelligence* che riguarda le minacce informatiche, fra le quali il legislatore fa rientrare anche la c.d. 'consapevolezza situazionale'; *iv*) a qualsiasi aspetto che richieda le competenze di tipo tecnico in materia di cibersicurezza proprie dello stesso CERT-EU[29]. Inoltre, quest'ultimo, nell'ambito delle sue competenze, intraprende una cooperazione (espressamente definita dal legislatore come "strutturata") con l'ENISA allo scopo di sviluppare capacità, una cooperazione di tipo operativo nonché analisi strategiche di lungo periodo rispetto alle minacce informatiche (secondo quanto disposto dal regolamento (UE) 2019/881). Il CERT-EU può altresì contare su una cooperazione, e conseguente scambio di informazioni, con il Centro per la lotta alla criminalità informatica di Europol[30].

Un ulteriore profilo, che si interseca con l'aspetto relativo alla cooperazione, attiene ai poteri riconosciuti al CERT-EU al fine di concorrere all'attuazione del regolamento (UE) 2023/2848. Il legislatore europeo attribuisce a tale organismo il potere di predisporre inviti ad intervenire il cui contenuto ha ad oggetto la descrizione delle misure di sicurezza urgenti che i soggetti dell'UE sono chiamati ad adottare nel termine prestabilito[31]. Inoltre, il CERT-EU può avanzare proposte al IICB per indirizzi destinati o a tutti i soggetti dell'UE ovvero solamente ad una parte di essi[32], nonché raccomandazioni – sempre rispetto al Comitato appena richiamato – da effettuare nei confronti di singoli soggetti dell'UE[33].

Prima di passare al profilo delle relazioni intersoggettive merita rapidamente analizzare il contenuto di tali indirizzi e regolamenti per mettere così in luce la tipologia di apporto che può derivare dal CERT-EU nell'opera di attuazione del presente regolamento. Il contenuto di questi atti, secondo quanto disposto, può prevedere, fra l'altro, metodologie comuni nonché un modello in grado

27 Sul punto, di recente, cfr. Moroni 2024; Giupponi 2024.

28 Art. 13, par. 3, lett. *f*).

29 Art. 13, par. 4, lett. *a*), *b*), *c*) e *d*).

30 Art. 13, par. 5. Sulla criminalità informatica, per un inquadramento generale, cfr. Pietropaoli 2022.

31 Art. 14, par. 1, lett. *a*), con l'aggiunta della previsione per cui il soggetto dell'UE interessato – dopo aver ricevuto l'invito ad adottare le misure di sicurezza urgenti ritenute necessarie – è tenuto tempestivamente ad informare il CERT-EU su come ha applicato le misure di sicurezza suggerite.

32 Art. 14, par. 1, lett. *b*).

33 Art. 14, par. 1, lett. *c*).

di valutare la maturità della cibersicurezza dei soggetti dell'UE[34], così come le modalità (o, comunque, i miglioramenti) che concernono la gestione dei rischi per la cibersicurezza e le relative misure di gestione dei rischi ad essa connessi[35]. Inoltre, tali indirizzi e raccomandazioni possono indicare anche le modalità afferenti alle valutazioni circa il livello di maturità della cibersicurezza[36] e gli accordi di condivisione delle informazioni sulla cibersicurezza[37], previsti dall'art. 20 del presente regolamento.

Per quanto riguarda più nel dettaglio l'aspetto relativo alla cooperazione, il regolamento (UE) 2023/2848 detta una serie di disposizioni aventi ad oggetto, da un lato, il profilo della cooperazione tra il CERT-EU e gli omologhi degli Stati membri e, dall'altro, la cooperazione fra il CERT-EU e gli omologhi diversi ed ulteriori dagli Stati membri.

Rispetto al primo versante, il CERT-EU è tenuto a cooperare e scambiare informazioni, senza ingiustificato ritardo, con gli omologhi degli Stati, giustappunto; più precisamente, il legislatore stabilisce che tale cooperazione e scambio di informazioni avvenga con gli CSRIT[38], ovvero, se necessario, con le autorità competenti e i c.d. 'punti di contatto unici'[39]. L'oggetto di ciò è rappresentato da incidenti, minacce informatiche, vulnerabilità, quasi incidenti, oltre che dalle possibili contromisure e le c.d. '*best practices*' e, più in generale, tutte le questioni ritenute pertinenti per migliorare la protezione degli ambienti TIC di tutti i soggetti dell'UE, e ciò anche per mezzo della rete CSIRT[40], istituita – lo si ricorda – al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri (c.d. 'rete dei CSIRT nazionali')[41].

Coerentemente con tale previsione si prevede poi che il CERT-EU comunichi tempestivamente agli omologhi pertinenti dello Stato in questione[42] l'incidente significativo di cui è venuto a conoscenza[43].

34 Art. 14, par. 2, lett. *a*).

35 Art. 14, par. 2, lett. *b*).

36 Art. 14, par. 2, lett. *c*). A tali valutazioni il regolamento (UE) 2023/2840 dedica un apposito articolo (7).

37 Art. 14, par. 2, lett. *f*).

38 Il riferimento è ai Team di risposta agli incidenti di sicurezza informatica (CSIRT) istituiti a norma dell'art. 10 della direttiva (UE) 2022/2555.

39 Punto di contatto che, secondo quanto disposto dall'art. 8 della direttiva (UE) 2022/2555, svolge una funzione di collegamento al fine di garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con quelle pertinenti degli altri Stati membri e, ove ritenuto opportuno, anche con la Commissione e l'ENISA; inoltre, al punto di contatto è attribuito il compito di garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro. Si ricorda, altresì, che tale disposizione prevede anche che, allorché uno Stato abbia designato solamente una autorità competente responsabile della cibersicurezza e dei relativi compiti di vigilanza, quella stessa autorità assuma pure il ruolo di punto di contatto (par. 3).

40 Art. 17, par. 1.

41 Il riferimento è all'art. 15 della direttiva (UE) 2022/2555 rubricato Rete CSIRT.

42 Ossia lo Stato nel cui territorio si è verificato l'incidente significativo.

43 Art. 17, par. 2.

Il legislatore europeo attribuisce al CERT-EU il potere di scambiare, "senza indebito ritardo" – così si legge – specifiche informazioni circa gli incidenti con i soggetti omologhi degli Stati membri allo scopo di facilitare il rilevamento delle minacce informatiche o degli incidenti analoghi e, più in generale, per poter fornire il proprio contributo rispetto all'analisi di quel determinato incidente, senza che sia necessario ricevere preventivamente la relativa autorizzazione da parte del soggetto dell'UE interessato. Per quanto concerne, invece, lo scambio di informazioni specifiche che abbiano ad oggetto la rivelazione dell'identità del bersaglio dell'incidente di cibersicurezza, il CERT-EU lo può fare solo a determinate condizioni, tipizzate dal legislatore: *i*) il soggetto dell'UE interessato deve rilasciare il proprio consenso; *ii*) il soggetto dell'UE interessato (cioè oggetto dell'incidente) non vi acconsente ma, tuttavia, la diffusione della sua identità avrebbe quale effetto quello di aumentare la probabilità di evitare o, comunque, attenuare ulteriori incidenti altrove[44]; *iii*) il soggetto dell'UE interessato dall'incidente ha già pubblicizzato il proprio coinvolgimento[45].

In relazione al profilo della cooperazione con gli altri omologhi, il legislatore specifica anzitutto che tale cooperazione con questi soggetti possa avvenire, purché essi rispettino i requisiti dell'UE in materia di cibersicurezza, precisando altresì che vi rientrano anche gli omologhi di specifici settori.

L'oggetto della cooperazione, in questi casi, attiene agli strumenti e ai metodi (come, per esempio, le tecniche, le tattiche, le procedure e le *best practices*) nonché alle minacce informatiche ed alle vulnerabilità. È richiesta l'approvazione preventiva da parte del IICB per poter procedere a qualsiasi tipo di cooperazione con i soggetti previsti e tale approvazione deve avvenire caso per caso. Una volta istituita questa cooperazione, il CERT-EU è tenuto ad informare gli omologhi dello Stato membro nel cui territorio si trova il soggetto con cui si è intrapresa siffatta cooperazione. Si stabilisce, inoltre, che tale cooperazione possa eventualmente inverarsi anche mediante accordi di riservatezza nella forma dei contratti e/o degli accordi amministrativi[46].

È importante sottolineare come ulteriori forme di cooperazione possano essere intrattenute, da parte del CERT-EU, con una serie di partner come, ad esempio, i soggetti commerciali (compresi quelli che appartengono a specifici settori), le or-

44 Il legislatore stabilisce, in questo caso, che le decisioni di scambiare informazioni siano avallate dal direttore del CERT-EU, descrivendone poi l'intera procedura.

45 Art. 17, par. 3.

46 Secondo quanto disposto dall'art. 18, par. 1, tali accordi di riservatezza non debbono essere preventivamente approvati ad opera del Comitato interistituzionale, pur dovendo, tuttavia, avvisare il suo presidente. Se dovesse ricorrere una situazione di imminente ed urgente necessità di scambiare informazioni circa la cibersicurezza nell'interesse dei soggetti dell'UE (o anche di altri soggetti), è possibile procedere a tale scambio purché questo avvenga con un soggetto dotato di competenze, capacità e conoscenze specifiche ritenute necessarie per far fronte a tale situazione di urgenza e ciò può verificarsi anche qualora il CERT-EU non abbia stipulato un accordo di riservatezza con tale soggetto; in questi casi, però, è richiesto al CERT-EU di procedere ad una comunicazione immediata al presidente del Comitato e di tenere informato lo stesso Comitato mediante relazioni e/o riunioni periodiche.

ganizzazioni internazionali, nonché enti nazionali di Stati non appartenenti all'UE o, addirittura, singoli esperti. Tale cooperazione, prevede il legislatore, è funzionale alla raccolta di informazioni riguardo a minacce informatiche (siano esse generali, siano esse specifiche), quasi incidenti, vulnerabilità e possibili contromisure. Se si ritiene opportuna una cooperazione di più ampia portata con tali soggetti è necessario che il CERT-EU chieda, caso per caso, un'approvazione preventiva al Comitato interistituzionale[47]. Inoltre, il CERT-EU, una volta ricevuto il consenso da parte del soggetto dell'UE interessato dall'incidente, e a condizione che sussista un accordo di non divulgazione con il soggetto omologo o con il partner interessato[48], può fornire ad essi le informazioni relative allo specifico incidente, e ciò con la sola giustificazione di contribuire alla sua analisi[49].

Un ultimo profilo su cui preme soffermare l'attenzione è quello concernente gli accordi di condivisione delle informazioni sulla cibersicurezza. Invero, com'è evidente, si tratta di un aspetto di particolare rilevanza – da salutare con favore al netto di una parziale 'timidezza' del legislatore, come si dirà – che va nella direzione di un rafforzamento del livello di cibersicurezza nei soggetti dell'UE, aumentando in questo modo la capacità di risposta dell'UE dinanzi agli attacchi informatici.

Il legislatore dispone, infatti, che i soggetti dell'UE, su base volontaria, possano notificare e fornire informazioni al CERT-EU in merito agli incidenti, alle minacce informatiche, ai quasi incidenti ed alle vulnerabilità che li interessano. Il CERT-EU è, a sua volta, tenuto a garantire la disponibilità di efficaci mezzi di comunicazione, dotati di un livello di tracciabilità, riservatezza e affidabilità elevati, proprio per rendere più agevole lo scambio e, soprattutto, la condivisione delle informazioni con i soggetti sopra menzionati. Si detta poi una specificazione nient'affatto irrilevante che incide sull'operatività dello stesso CERT-EU; infatti, si prevede che quest'ultimo, nel trattare le notifiche pervenutegli, possa dare priorità a quelle obbligatorie, prendendo successivamente in considerazione le notifiche volontarie. In relazione a quest'ultima tipologia di notifica, il legislatore afferma che – salvo ovviamente il caso delle notifiche derivanti dal controllo del IICB circa l'osservanza del presente regolamento[50] – esse non debbono comportare, per il soggetto che le effettua, nessun tipo di obbligo ulteriore rispetto a quelli a cui è già sottoposto abitualmente[51].

Inoltre, si riconosce al CERT-EU il potere di chiedere ai soggetti dell'UE le informazioni "tratte dai loro rispettivi inventari dei sistemi TIC", incluse quelle relative alle minacce informatiche, ai quasi incidenti, alle vulnerabilità, nonché quelle attinenti ai c.d. 'indicatori di compromissione', agli allarmi di cibersicurezza ed alle raccomandazioni che riguardano la configurazione stessa degli strumenti di cibersicurezza, per poterne così rilevare gli incidenti. Il soggetto che riceve la domanda

47 Art. 18, par. 2.
48 Il riferimento è ai soggetti di cui ai paragrafi 1 e 2 dell'art. 18.
49 Art. 18, par. 3.
50 Il riferimento è all'art. 10.
51 Art. 20, par. 1.

di trasmissione delle informazioni è tenuto ad inviarla senza ritardo, così come gli è richiesto di procedere ad ogni loro eventuale successivo aggiornamento[52].

Si tratta, com'è agevole intuire (e come chiarisce, del resto, il legislatore), di un potere che, in ultima analisi, è imprescindibile per il CERT-EU affinché sia in grado di realizzare i compiti che gli sono stati espressamente attribuiti mediante il regolamento in esame.

Anche le informazioni specifiche circa un determinato incidente che rivelano l'identità stessa del soggetto dell'UE coinvolto nell'incidente possono essere oggetto di scambio, purché sussista il consenso di quest'ultimo; il quale può pure rifiutarsi di prestare il proprio consenso, essendo tuttavia tenuto in tal caso a spiegare al CERT-EU le ragioni alla base del suo diniego[53].

Si stabilisce poi, da un lato, che i soggetti dell'UE condividano sia con il Parlamento europeo che con il Consiglio, su loro richiesta, le informazioni riguardanti il completamento dei piani di cibersicurezza[54], quegli stessi piani rispetto ai quali il presente regolamento dedica un'apposita disposizione e, dall'altro, similmente, che il CERT-EU ovvero il IICB (a seconda dei casi), condividano – sempre con i due organi appena menzionati e sempre previa richiesta – indirizzi, raccomandazioni ed inviti ad agire[55].

4. (*Segue*). Le relazioni intersoggettive e l'esigenza di coordinamento

Il profilo relativo al coordinamento riveste notevole importanza poiché – come noto, ed in parte visto – molteplici sono i soggetti a livello europeo (e, quindi, a livello nazionale) chiamati, a vario titolo, a concorrere a quello che si può qui definire nei termini di 'governo della cibersicurezza'. Pertanto, appare necessario riflettere circa le relazioni che sussistono fra tali soggetti e su come si possa assicurare il coordinamento fra di loro, strumentale a configurare un sistema realmente in grado di regolare la cibersicurezza ed aumentarne il relativo livello nei soggetti dell'UE, che si rende tanto più necessario proporzionalmente all'aumentare sia degli attacchi informatici che del loro grado di raffinatezza.

Ai presenti fini interessa, in particolare, tentare di delineare le relazioni che sussistono fra il IICB, il CERT-EU e l'ENISA. Da questo punto di vista, si può prendere in considerazione il coordinamento (e conseguente cooperazione) che il legislatore europeo, con il presente regolamento, ha inteso prevedere rispetto alla risposta in caso di incidenti.

Il CERT-EU, infatti, svolgendo una funzione analoga a quella di una piattaforma creata per lo scambio di informazioni in materia di cibersicurezza e susseguente coordinamento della risposta allorché si verifichi un incidente, è tenuto a rendere più agevole la circolazione delle informazioni attinenti agli incidenti, alle minacce

52 Art. 20, par. 2.
53 Art. 20, par. 3.
54 Art. 20, par. 4.
55 Art. 20, par. 5.

informatiche, alle vulnerabilità e ai quasi incidenti. Questa circolazione – si legge – deve avvenire fra i soggetti dell'UE nonché con i soggetti omologhi degli Stati membri dell'UE (quelli previsti dall'art. 17 per intendersi) e gli altri soggetti omologhi (quelli di cui all'art. 18)[56].

Il CERT-EU può facilitare tale coordinamento fra i soggetti dell'UE in materia di risposta agli incidenti anche per mezzo di una stretta cooperazione con l'ENISA e, per fare ciò, può ricorrere ad una serie di 'strumenti' come, a titolo di esempio, il sostegno reciproco mediante la condivisione delle informazioni ritenute pertinenti per i soggetti dell'UE ovvero attraverso la fornitura di assistenza[57]. Sempre potendo ricorrere ad una stretta cooperazione con l'ENISA, il CERT-EU sostiene i soggetti dell'UE con riferimento alla 'consapevolezza situazionale' degli incidenti, delle minacce, delle vulnerabilità e dei quasi incidenti. Inoltre, il CERT-EU condivide gli sviluppi che si sono prodotti nel settore della cibersicurezza[58].

Nell'attività di coordinamento di tali incidenti un ruolo importante è attribuito anche al IICB perché è a questi che spetta il compito – sulla base di una proposta del CERT-EU – di adottare gli atti e gli indirizzi sul coordinamento della risposta in caso di incidenti, oltre che sulla cooperazione allorché si verifichino incidenti più gravi. Il CERT-EU, inoltre, è tenuto a fornire una consulenza rispetto a come debba essere segnalato l'incidente alle autorità competenti, segnalazione che deve avvenire senza ritardo e che è la conseguenza di un incidente rispetto al quale sussiste un sospetto circa la sua rilevanza ai termini della legge penale[59].

Ancora più evidente è la cooperazione fra i tre soggetti in questione se si esamina la disposizione inerente la gestione degli incidenti più gravi. Invero, in questo caso, si ha una più stretta relazione fra il IICB da un lato e il CERT-EU e l'ENISA dall'altro; il primo, come già anticipato, ha il potere di istituire un piano di gestione delle crisi informatiche per far fronte agli incidenti e ciò avviene in stretta cooperazione – così si legge – con il CERT-EU e l'ENISA[60]. Anche in tali casi il soggetto deputato al coordinamento è sempre il CERT-EU, il quale è chiamato altresì ad assistere proprio il IICB nel coordinamento di quegli stessi piani a cui si è appena fatto riferimento[61].

Più in generale, si può osservare come il Comitato, nei confronti del CERT-EU – lo si vedrà meglio più avanti – abbia un potere sia di vigilanza, dato che ne controlla costantemente l'attuazione delle priorità e degli obiettivi, che di natura direttiva, potendo infatti imprimere a quest'ultimo – lo si è già anticipato – una "direzione strategica". Il Comitato è, dunque, titolare di un rilevante potere di coordinamento del CERT-EU che si esplica anche mediante la facoltà di fornire orientamenti al suo direttore. Con riferimento, invece, ai rapporti con l'ENISA, il Comitato può farsi sostenere da essa nell'opera di scambiare le *best practices* nonché le informa-

56 Art. 22, par. 1.
57 Art. 22, par. 2.
58 Art. 22, par. 3.
59 Art. 22, par. 4.
60 Art. 23, par. 1.
61 Art. 23, par. 3.

zioni relative all'attuazione del regolamento (UE) 2023/2848. Inoltre, come visto, l'ENISA è rappresentata in seno al Comitato e ciò proprio in ragione del suo ruolo quale centro di competenza in materia di cibersicurezza e del sostegno che, più in generale, tale autorità fornisce ai soggetti dell'UE.

Sussistono poi rapporti diretti fra CERT-EU e ENISA. Il primo, infatti, dovrebbe avvalersi delle competenze dell'ENISA sulla base di quella cooperazione strutturata sancita espressamente dal regolamento (UE) 2019/881, dove, per converso, si prevede che quest'ultima si avvalga delle competenze, sia tecniche che operative, disponibili del CERT-EU, attraverso, appunto, tale cooperazione strutturata, cooperazione che potrebbe fondarsi sulle competenze proprie dell'ENISA, con la possibilità (anche) di ricorrere ad accordi fra i due soggetti allo scopo di definire l'attuazione in concreto di questa forma di cooperazione ed evitare così la duplicazione delle relative attività[62].

Il regolamento (UE) 2023/2841 ricorda, infatti, la possibilità di definire accordi fra tali due soggetti, sottolineando, in particolare, la cooperazione che il CERT-EU potrebbe instaurare con l'ENISA in punto di analisi delle minacce, condividendo con quest'ultima (con cadenza periodica) la sua relazione avente ad oggetto la panoramica in tema di minacce[63].

Emerge, dunque, in maniera piuttosto evidente, l'esigenza di coordinamento[64] fra questi tre soggetti che, a vario titolo, concorrono al governo della cibersicurezza ed alla loro regolazione, nella direzione del rafforzamento del livello complessivo di cibersicurezza nei soggetti dell'UE.

Il IICB si inserisce in un assetto che già vedeva la presenza sia del CERT-EU che dell'ENISA e, proprio in virtù della sua organizzazione che è preordinata a rappresentare tutti i soggetti dell'UE in qualche misura interessati alla (e dalla) cibersicurezza, rafforza tale assetto mediante la capacità di coordinamento che le è propria.

Si potrebbe, pertanto, configurare una sorta di 'triade' nel governo e quindi nella regolazione della cibersicurezza, dove, accanto all'ENISA e al CERT-EU, si affianca ora il Comitato[65]. L'ENISA continua a svolgere il suo ruolo tradizionale di soggetto che, anzitutto, è chiamato a "conseguire un elevato livello comune di cibersicurezza in tutta l'UE, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'UE nel miglioramento della cibersicurezza". Il CERT-EU, anche in ragione dei maggiori compiti e del rafforzamento organizzativo recentemente operato dal legislatore europeo, costituisce – per così dire – il 'braccio armato' sia dell'ENISA che del Comitato, svolgendo un ruolo prevalentemente operativo, fondamentale al contrasto e, prima ancora, alla prevenzione degli attacchi informatici.

Il Comitato, in tutto ciò, rappresenta uno strumento di particolare importanza poiché mira a definire un livello (elevato) di cibersicurezza comune tra i sogget-

62 Punto 33 dei *Considerando* del regolamento (UE) 2019/881.

63 Punto 32 dei *Considerando*.

64 Sull'importanza del coordinamento quale metodo "aperto" fra il piano europeo e quello nazionale cfr. Del Gatto 2012.

65 Si potrebbe parlare, da questo punto di vista, di una sorta di "arcipelago amministrativo".

ti dell'UE, sul presupposto per cui, avendo il regolamento anche l'obiettivo di rafforzare il livello complessivo di cibersicurezza dell'UE – coerentemente con quanto già previsto dalla direttiva (UE) 2022/2555 –, tale rafforzamento debba riguardare tutti i soggetti dell'UE in maniera uniforme ed indiscriminata. Invero – come ricorda lo stesso legislatore – gli ambienti TIC di quest'ultimi sono fortemente interdipendenti fra loro[66], cosicché qualsiasi attacco ad un soggetto potrebbe avere effetti assai dannosi anche su uno o più degli altri soggetti appartenenti all'UE.

In altre parole, il rafforzamento del livello di cibersicurezza dei soggetti all'interno dell'UE deve riguardarli tutti, altrimenti rischia di essere un'operazione vana, fine a sé stessa, che dinanzi ad un attacco informatico di vaste dimensioni e raffinata sofisticatezza potrebbe mandare in tilt l'intero sistema (informatico) europeo e pregiudicare così i diritti da esso dipendenti.

5. La direzione strategica del CERT-EU ed un nuovo potenziale modello regolatorio all'orizzonte

Il potere del Comitato di vigilare in relazione alla realizzazione delle priorità nonché degli obiettivi generali del 'CERT-EU', con la possibilità di imprimere a tale centro una direzione di tipo strategico, offre interessanti spunti per riflettere sul modello regolatorio della cibersicurezza che va delineandosi[67]. Invero, avuto particolare riguardo alla possibilità di imprimere al CERT-EU una direzione di tipo strategico, sembra aprirsi la strada per un modello di regolazione della cibersicurezza che si può definire nei termini di 'regolazione strategica'. Come noto, infatti, nel 2020 è stata adottata la strategia sulla cibersicurezza[68], con l'obiettivo di configurare una rete internet globale ed aperta, contraddistinta da linee guida per poter affrontare i rischi sia per la sicurezza che per i diritti e le libertà fondamentali dei cittadini dell'UE. La strategia definisce, quindi, in quale modo l'UE proteggerà i suoi cittadini, le imprese e le istituzioni dalle minacce informatiche, come promuoverà la cooperazione internazionale e, infine, secondo quali azioni contribuirà a garantire una rete internet globale ed aperta.

In questa sede non interessa analizzare la strategia in sé quanto, diversamente, mettere in luce come essa possa costituire il substrato per configurare il modello di regolazione di tipo strategico. Tale strategia, lo si ricorda, si colloca in quel variegato panorama di documenti europei – composto dal documento "Plasmare il futuro

66 Utilizzano, infatti, flussi di dati integrati e, inoltre, sono accomunati dalla circostanza di essere caratterizzati da una stretta collaborazione fra i loro utenti.

67 Sul punto, con specifico riguardo alla regolazione delle piattaforme digitali, dove si effettuano osservazioni (circa i diversi modelli regolatori) in grado di offrire spunti utili per la configurazione del modello regolatorio della cibersicurezza, secondo una prospettiva che muove dal presupposto della necessità di considerare l'intero sistema digitale come l'oggetto (e, quindi, l'ambito) dei nuovi modelli di regolazione delle piattaforme, cfr. Santaniello 2021.

68 JOIN (2020) 18 final.

digitale dell'Europa"[69], dal piano per la ripresa europea della Commissione[70], dalla strategia per l'Unione della sicurezza 2020-2025[71] e, infine, dalla strategia globale per la politica estera e di sicurezza dell'Unione europea – e mira ad esserne, come si legge, "una componente chiave".

Il Comitato, si è detto, imprime al CERT-EU una direzione strategica attraverso i compiti che gli sono espressamente assegnati dal legislatore. Di particolare rilievo sotto questo profilo sono, fra gli altri, il potere di fornire orientamenti al direttore del CERT-EU e il potere di approvare il suo programma di lavoro annuale, controllandone la relativa attuazione. Il Comitato, lo si ricorda, adotta una strategia pluriennale al fine di innalzare il livello di cibersicurezza nei soggetti dell'UE, a cui si accompagna una sua valutazione periodica e, soprattutto, la possibilità di procedere ad una sua modifica.

Si tratta, pertanto, di una regolazione che sembra essere una 'regolazione strategica', vale a dire una regolazione che si fonda anzitutto su una strategia, senza per questo essere però caratterizzata da misure specifiche individuate *ex ante* dal legislatore. Non è la regolazione tradizionale conosciuta dal diritto amministrativo in passato e, più in generale, dal diritto della regolazione, quella cioè che si basava su strumenti di c.d. '*command and control*', dove non c'era una strategia alla base e le misure della regolazione erano specificamente (e preventivamente) previste dal legislatore.

L'obiettivo della regolazione di questo tipo consiste nell'attuazione della strategia: è questa che fissa il macro-obiettivo (che, in tal caso, è, appunto, quello di innalzare il livello di cibersicurezza nei soggetti dell'UE) e la regolazione è lo strumento che serve per attuarlo in concreto. Si è in presenza di una regolazione flessibile poiché è la stessa strategia che si può aggiornare periodicamente e, di conseguenza, è una regolazione caratterizzata da un possibile mutamento in punto di strumenti di cui servirsi per conseguire l'obiettivo finale (questo, in teoria, non flessibile); essi, infatti – lo si ripete –, non sono predeterminati dal legislatore.

Tale modello regolatorio ha degli elementi in comune con la c.d. 'regolazione persuasiva', la quale, non a caso, "si definisce in relazione agli obiettivi piuttosto che agli strumenti"[72]. Invero, è l'obiettivo stabilito dalla strategia che contraddistingue e caratterizza la regolazione flessibile. La regolazione persuasiva è, del resto, una regolazione flessibile, una regolazione che – come è stato osservato – "può consentire una maggiore rapidità nell'adattamento alle acquisizioni della scienza"[73].

Ciò detto, la regolazione strategica non è necessariamente – e non deve essere – una regolazione per così dire '*soft*', 'debole', potendo, al contrario, essere una regolazione 'forte'. La sua 'forza' (nel senso di vincolatezza) dipende sia dal tasso di ambizione degli obiettivi posti che dai termini prefissati entro i quali conseguire siffatti obiettivi, oltre che, ovviamente, dagli strumenti utilizzati.

69 COM(2020) 67 final.
70 COM(2020) 98 final.
71 COM(2020) 605 final.
72 Cafaggi, 2022: 494.
73 Cafaggi, 2022: 521.

Tale modello di regolazione è – e non potrebbe essere altrimenti – multilivello e deve necessariamente superare l'attuale situazione caratterizzata da un eccesso di norme, la cui causa è da rinvenire (anche) in quel fenomeno che assume il nome di 'normazione policentrica'. All'opposto, le norme devono essere quelle strettamente necessarie al raggiungimento dell'obiettivo fissato dal legislatore nelle varie strategie. L'orizzonte della regolazione multilivello è indispensabile in ragione della rilevanza globale del fenomeno della cibersicurezza e, perciò, è essenziale il coinvolgimento del livello sovra-europeo. Per quanto riguarda invece il discorso circa l'esigenza di superare l'eccesso di norme, ciò dipende dal continuo e rapido mutamento delle tecnologie e, quindi, degli attacchi informatici; un numero elevato di norme mal si presterebbe alla prevenzione ed al contrasto di tali attacchi, anche perché la promulgazione di esse richiede un lasso di tempo, a partire dalla loro formulazione[74], che difficilmente consentirebbe la prevenzione dei rischi informatici, oltre che per il fatto che, comunque, un eccesso di norme crea, come noto, confusione, anche rispetto a quale norma dover applicare e a come poi 'coordinarle' fra di loro.

Tutto ciò ha delle implicazioni evidenti sulle amministrazioni[75], destinate a vedere aumentare la loro discrezionalità; l'attività delle amministrazioni, infatti – non eccessivamente imbrigliate nelle maglie del legislatore –, può consentire quella 'capacità adattiva' al mutamento delle tecnologie e degli attacchi informatici; certo, ciò presuppone, comunque, il rispetto del principio di legalità e, di conseguenza, il mantenimento di quel legame con l'apparato politico, necessario ai fini della loro legittimazione (democratica). Inoltre, è essenziale che tali amministrazioni siano titolari delle competenze tecniche richieste (nonché degli strumenti) per poter predisporre una regolazione efficace, e cioè tempestiva e tecnica.

Si tratta di una regolazione che, non potendo prescindere anche dai soggetti privati[76], lascia inevitabilmente un margine di libertà a quest'ultimi, secondo un meccanismo che – come già sottolineato – non sembra essere del tipo *top down*, e, dunque, eteroimposto, ma congiunto, sulla base di un obiettivo comune che si tenta di raggiungere 'incentivando' l'adozione di una serie di misure poiché all'assunzione di esse consegue un vantaggio per tutti coloro i quali decidono di attuarle[77]. Un modello regolatorio che, per la verità – anche alla luce dell'ultima

74 Anche se, sotto questo profilo, la digitalizzazione dei relativi procedimenti legislativi potrebbe contribuire ad una riduzione dei tempi; sul punto, con riferimento al piano nazionale (ma le cui considerazioni possono estendersi anche al piano europeo), cfr. le osservazioni di Cavalli 2023; Ibrido 2022. In merito, avuto particolare riguardo agli algoritmi, in una prospettiva di ampio respiro tesa a riflettere sulle implicazioni che tutto ciò determina per il modello attuale – sempre più messo in discussione – di democrazia rappresentativa, Cardone 2022.

75 In proposito, con particolare riguardo alla cibersicurezza nelle amministrazioni digitali, cfr. Montessoro 2019.

76 Nella prospettiva della necessaria collaborazione fra 'pubblico' e 'privato' ai fini della gestione dei rischi informatici cfr. Previti 2022. Sulla necessità di rafforzare la collaborazione fra 'pubblico' e 'privato' cfr. anche Bruno 2020.

77 Non si tratta della regolazione per incentivi di tipo tradizionale; in tal caso, quello che si definisce 'incentivo' non è un vantaggio attribuito dal legislatore, esterno cioè alla sfera giu-

considerazione circa l'impossibilità di prescindere dai soggetti privati – non è estraneo all'ordinamento europeo, il quale, da anni, attribuisce centralità allo strumento della strategia, strumento che, più di recente, ha assunto un'importanza (e, soprattutto, un'attenzione) con la comunicazione nota come *Green deal* europeo[78]. Ecco, si tratta di una regolazione – quella strategica in materia di cibersicurezza – non così dissimile da quella propria del *Green Deal* europeo; anzi, sembrano sussistere una serie di punti di contatto fra le due, e ciò non deve destare stupore poiché entrambe si innestano in quel processo di transizione (ecologica e digitale)[79] che caratterizza la politica europea più recente e riprova del collegamento fra il *Green deal* e la cibersicurezza è rappresentato dal fatto che la strategia relativa a quest'ultima –coerentemente proprio con lo stesso *Green Deal* – secondo la Commissione europea è "essenziale per la transizione verso un'energia più pulita, attraverso reti transfrontaliere e contatori intelligenti, evitando inutili duplicazioni nell'archiviazione dei dati"[80].

La regolazione strategica, dunque, è una regolazione di tipo flessibile e ciò le consente di adattarsi perfettamente (quantomeno da un punto di vista teorico) alla cibersicurezza ed al suo oggetto, essendo coerente con i repentini mutamenti che interessano le nuove tecnologie, di cui deve inevitabilmente farsi carico la cibersicurezza e, con essa, il diritto che la intende regolare.

6. Osservazioni conclusive

La cibersicurezza, come noto, non è solamente una questione di 'difesa nazionale' ma anche e, soprattutto, una questione legata ai diritti, da intendere più precisamente nei termini di 'fruizione dei diritti fondamentali di ciascun individuo'. Pertanto, si pone l'esigenza di una sua solida regolazione pubblica[81] per far fronte ai rischi sempre più frequenti (la 'società del rischio') che caratterizzano ormai la

ridica del destinatario, ma, diversamente, coincide con il rafforzamento di un interesse di cui il destinatario della misura è titolare e che è, quindi, già nella sua sfera giuridica. Il legislatore non concede, pertanto, un incentivo, un vantaggio, ma – previa definizione dell'obiettivo finale da raggiungere – si limita ad individuare le modalità attraverso le quali i destinatari possono conseguire quel determinato obiettivo. Sul punto cfr. Valaguzza 2016. Per un inquadramento generale sul ruolo della regolazione nel campo del diritto amministrativo, per tutti, cfr. Stewart 2004.

78 Sul *Green Deal* europeo quale processo regolatorio, per primo, Chiti 2022.

79 Sulle c.d. 'transizioni gemelle', cfr. Camisa 2024; Franca, Porcari, Sulmicelli 2024.

80 JOIN (2020) 18 final, 4. Sui dati, di recente, nell'ambito di una prospettiva che muove da un mutamento di paradigma nella regolazione europea avente ad oggetto i dati, con spunti circa il riutilizzo degli stessi, cfr. Cremona 2023.

81 Sulle implicazioni per i poteri pubblici nell'epoca della rivoluzione digitale, caratterizzata dalla potente presenza di poteri privati, cfr. Mannoni, Stazi 2021. Con particolare riferimento ai poteri privati ed al relativo potere digitale cfr. Simoncini 2017; Betzu 2022; Ferrarese 2022; Cremona 2023; Pollicino 2023; Resta 2023; Cipolloni 2024. Sui poteri privati ed il nuovo modello regolatorio che sembra emergere alla luce, in particolare, di talune recenti normative adottate in ambito europeo (come, per esempio, il *Digital Markets Act* ed il *Digital Services Act*), cfr. Bruti Liberati 2023.

c.d. 'vita digitale'[82] di ogni essere umano, dove si assiste, per esempio, ad attacchi a sistemi[83] rendendoli inutilizzabili e, quindi, impedendo l'esercizio di funzioni pubbliche o l'erogazione di prestazioni circa servizi essenziali, con la conseguente lesione (o rischio di lesione) di quegli stessi diritti fondamentali[84] riconosciuti e garantiti dall'ordinamento europeo (e dalle relative costituzioni) che, ormai, costituiscono il 'punto logico di partenza' di ogni analisi correttamente impostata sulla cibersicurezza, e la regolazione (forse quella che si è qui definito come 'regolazione strategica') deve muoversi in questa direzione, sebbene il cammino sia ancora lungo e dai risultati in larga parte incerti.

Ciò che invece appare certo è che la riflessione sul punto – con riferimento dunque, in particolare, al IICB – passi inevitabilmente da una più solida cooperazione fra i vari organismi deputati alla regolamentazione[85] e ad alla regolazione del fenomeno della cibersicurezza allo scopo di concorrere unitamente, ed in ultima analisi, alla garanzia di quei diritti ad essa connessi ed il cui effettivo godimento rischia di essere sempre più posto in costante e forte discussione.

Infine, prima di concludere – pur essendo estraneo al presente contributo il profilo concernente direttamente il governo della cibersicurezza – sembra possibile osservare che l'istituzione del Comitato, unitamente ai nuovi poteri attribuiti al CERT-EU, sono destinati a segnare una parziale riconfigurazione dell'assetto di governo della cibersicurezza a livello europeo (e quindi, in parte, anche a livello nazionale)[86] secondo una direttrice che appare essere caratterizzata dall'idea di fondo di una regolazione più incisiva per far fronte ai mutamenti in atto, sempre più frequenti, che interessano le nuove tecnologie e, in particolare, gli attacchi informatici, i quali rappresentano sicuramente una delle minacce[87] più serie e pericolose con le quali le società del 'domani' saranno inevitabilmente chiamate a confrontarsi.

Al diritto[88] il compito di cercare di anticipare tali rischi e, contestualmente – per quello che qui più interessa –, di ordinare il complesso ed articolato fenomeno della cibersicurezza, sulla scia di quell'autorevole insegnamento (ancora estremamente attuale) del diritto come strumento ordinante la società[89], dove l'ordine si con-

82 Nell'ambito di quella che si definisce ormai come "società digitale"; sul punto cfr. le riflessioni di Longo 2023. Sulla "società digitale" cfr. anche di Carpegna Brivio 2024. Con particolare attenzione al profilo dei diritti Celotto 2023.

83 Sulla sicurezza delle infrastrutture informatiche, di recente, cfr. Serini 2023. Più in generale, sulla sicurezza nel ciberspazio, cfr. Ursi 2023, dove si avanza l'ipotesi della sicurezza cibernetica quale (nuova) funzione pubblica.

84 In proposito, di recente, cfr. Iannuzzi, Laviola 2023.

85 Una recente ricognizione dell'evoluzione della disciplina in materia di cibersicurezza è offerta da Longo 2024. Cfr. anche Brighi 2024; Contaldo, Mula 2020.

86 Con una serie di implicazioni rispetto all'Agenzia nazionale per la cybersecurity, sulla quale, fra i tanti, Forgione 2022.

87 Con specifico riferimento al versante dei reati informatici cfr. Pietropaoli 2022.

88 In particolare quello pubblico; sul futuro e le sfide del diritto pubblico cfr. Aa.Vv. 2024.

89 Il riferimento è, e non potrebbe essere altrimenti, al magistero di Paolo Grossi.

trappone (anteponendosi) al caos[90], che è il regno del più forte, il luogo ove, per definizione, non vi è spazio per i diritti, per quegli stessi diritti che, come si è detto, costituiscono ormai patrimonio essenziale ed insopprimibile della cibersicurezza.

Bibliografia

Aa.Vv. 2024, "Il futuro del diritto pubblico. Il tempo e le sfide", in *Diritto pubblico*, 1: 3-130.

Betzu M. 2022, *I baroni del digitale*, Napoli: Editoriale scientifica.

Brighi R., Chiara P.G. 2021, "La cybersicurezza come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea", in *Federalismi.it*, 21: 18-42.

Brighi R. 2024 [2021], "Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione", in T. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, Milano: Wolters Kluwer: 75-88.

Bruno B. 2020, "Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *Federalismi.it*, 14: 11-45.

Bruti Liberati E. 2023, "Poteri privati e nuova regolazione pubblica", in *Diritto pubblico*, 1: 285-301.

Cafaggi L. 2022, "Proibire, permettere, persuadere. Appunti di viaggio nella regolazione contemporanea", in *Mercato concorrenza e regole*, 3: 491-522.

Camisa F. 2024, "Ambiente e tecnologia: l'interconnessione tra le 'transizioni gemelle'", in *Federalismi.it*, 14: 55-75.

Camisa F., Simoncini A. 2024, "Il fattore umano e la regolazione della cybersecurity", in *Mondo digitale*, marzo: 1-17.

Cardone A. 2022, "Algoritmi e ICT nel procedimento legislativo: quale sorta per la democrazia rappresentativa?", in *Osservatorio sulle fonti*, 2: 57-382.

Caterina E. 2023, *Personalismo vivente. Origini ed evoluzione dell'idea personalista dei diritti fondamentali*, Napoli: Editoriale Scientifica.

Cavalli L. 2023, "Le Camere nell'emergenza da Covid-19. Notazioni ricostruttive e spunti problematici", in *Federalismi.it*, 3: 212-227.

Celotto A. 2023, *"Sudditi". Diritti e cittadinanza nella società digitale,* Milano: Giuffrè.

Chiti E. 2022, "Managing the ecological transition of the EU: the European green deal as a regulatory process", in *Common Market Law Review*, 59: 19-48.

Chiti E. 2009, "An important part of the EU's institutional machinery: features, problems and perspectives of European Agencies", in *Common Market Law Review*, 46: 1395-1442.

Chiti E. 2002, *Le Agenzie europee. Unità e decentramento nelle amministrazioni comunitarie*, Padova: Cedam.

Cipolloni C. 2024, *Persona, poteri privati e Stato nella rivoluzione internettiana*, Torino: Giappichelli.

Contaldo A., Mula D. (a cura di) 2020, Cybersecurity law. *Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica.

90 Da intendere nel senso di 'anomia', non (come sovente accade) di 'anarchia'. Sull'anarchia della Rete cfr. Gatti 2019.

Cremona E. 2023, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli: Edizioni Scientifiche Italiane.
Cremona E. 2023, "Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso", in *Rivista italiana di informatica e diritto*, 2: 111-130.
Del Gatto S. 2012, *Il metodo aperto di coordinamento. Amministrazioni nazionali e amministrazione europea*, Napoli: Jovene.
di Carpegna Brivio E. 2024, *Pari dignità sociale e* Reputation scoring*. Per una lettura costituzionale della società digitale*, Torino: Giappichelli.
Ferrarese M.R. 2022, *Poteri nuovi. Privati, penetranti, opachi*, Bologna: Il Mulino.
Forgione I. 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*, 4: 1113-1143.
Franca S., Porcari A., Sulmicelli S. (a cura di) 2024, *Le transizioni e il diritto. Atti delle giornate di studio 21-22 settembre 2023*, Napoli: Editoriale scientifica.
Gatti A. 2019, "Istituzioni e anarchia nella Rete. I paradigmi tradizionali della sovranità alla prova di Internet", in *Il diritto dell'informazione e dell'informatica*, 3: 711-743.
Giupponi T.F. 2024, "Il governo nazionale della cibersicurezza", in *Quaderni costituzionali*, 2: 277-304.
Iannuzzi A. 2023, "Paradigmi normativi per la disciplina della tecnologia: auto-regolazione, co-regolazione ed etero-regolazione", in *Bilancio, comunità, persona*, 2: 91-107.
Iannuzzi A., Laviola F. 2023, "I diritti fondamentali nella transizione digitale fra libertà e uguaglianza", in *Diritto costituzionale*, 1: 9-40.
Ibrido R. 2022, "Evoluzioni tecnologiche o involuzioni costituzionali? La 'reingegnerizzazione' del processo di decisione parlamentare", in *Osservatorio sulle fonti*, 2: 291-310.
Lalli A. (a cura di) 2024, *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, Torino: Giappichelli.
Longo E. 2024, "La disciplina della cybersecurity nell'Unione europea e in Italia", in F. Pizzetti, M. Orofino, A. Iannuzzi, S. Calzolaio, E. Longo (a cura di), *La regolazione europea della società digitale*, Torino: Giappichelli: 203-234.
Longo E. 2023, "La ricerca di un'antropologia costituzionale della società digitale", in *Rivista italiana di informatica e diritto*, 2: 147-160.
Mannoni S., Stazi G. 2021, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli: Editoriale scientifica.
Montessoro P.L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Istituzioni del Federalismo*, 3: 783-800.
Moroni L. 2024, "La governance della cybersicurezza a livello interno ed europeo: un quadro intricato", in *Federalismi.it*, 14: 179-199.
Pietropaoli S. 2022, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino: Giappichelli.
Pollicino O. 2023, "Potere digitale", in *Potere e Costituzione*, diretto da M. Cartabia, M. Ruotolo, *I tematici dell'Enciclopedia del diritto*, V, Milano: Giuffrè: 410-445.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it*, 25: 65-93.
Resta G. 2023, "Poteri privati e regolazione", in *Potere e Costituzione*, diretto da M. Cartabia, M. Ruotolo, *I tematici dell'Enciclopedia del diritto*, V, Milano: Giuffrè: 1008-1032.
Santaniello M. 2021, "La regolazione delle piattaforme e il principio della sovranità digitale", in *Digital Politics*, 3: 579-600.
Savino M. 2005, *I Comitati dell'Unione europea. La collegialità amministrativa negli ordinamenti compositi*, Milano: Giuffrè.

Serini F. 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*, 2: 41-76.
Simoncini A. 2022, "La co-regolazione delle piattaforme digitali", in *Rivista trimestrale di diritto pubblico*, 4: 1031-1049.
Simoncini A. 2017, "Sovranità e potere nell'era digitale", in O. Pollicino, T. E. Frosini, E. Apa (a cura di), *Diritti e libertà in Internet*, Milano: Mondadori Education.
Stewart R.B. 2004, "Il diritto amministrativo nel XXI secolo", in *Rivista trimestrale di diritto pubblico*, 1: 1-29.
Ursi R. (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli.
Valaguzza S. 2016, "La regolazione strategica dell'Autorità Nazionale Anticorruzione", in *Rivista della regolazione dei mercati*, 1: 9-58.

Carla Maria Saracino

Cybersecurity e mobilità intelligente: il binomio sicurezza/responsabilità

Abstract: Lo stato dell'arte europeo in ordine ai sistemi di trasporto intelligente risente delle diverse velocità di adeguamento degli Stati alle Direttive e agli atti di programmazione europei e dalla diversa sensibilità al fenomeno della mobilità sicura, digitale ed eco-integrata. Trattandosi di un tema che, inevitabilmente, coinvolge gli ambiti del diritto della sicurezza, dell'innovazione e dell'ambiente, lo studio si propone di indagarne tre aspetti fondamentali: la necessità di una regolamentazione del settore che necessita di una regolamentazione puntuale, di parametri applicativi e coordinate chiare; il connubio tra sicurezza individuale e appalti per l'innovazione, nelle forme del partenariato per l'innovazione e dei contratti di ricerca e sviluppo; la regolamentazione dei profili di responsabilità connessi, nonché la tutela dei *big data* e degli algoritmi che supportano i sistemi di mobilità sostenibili. In tali ambiti, avrà senso indagare l'atteggiarsi del potere regolatorio pubblico in relazione alle fattispecie di trasporto automatizzato.

Keywords: Mobilità intelligente; Innovazione; Cybersicurezza; Regolazione; Responsabilità.

1. Premessa

Lo stato dell'arte europeo in ordine ai sistemi di trasporto intelligente risente delle diverse velocità di adeguamento degli Stati alle Direttive e agli atti di programmazione europei e dalla diversa sensibilità al fenomeno della mobilità sicura, digitale ed eco-integrata. Trattandosi di un tema che, inevitabilmente, coinvolge gli ambiti del diritto della sicurezza, dell'innovazione e dell'ambiente, ci si propone di indagarne tre aspetti fondamentali.

In primo luogo, la disamina intenderà soffermarsi sulla necessità di una regolamentazione t*ough* del settore che necessita, più che di raccomandazioni e linee guida non vincolanti ascrivibili nel *soft law*, di una regolamentazione puntuale, di parametri applicativi e coordinate chiare per l'introduzione e, poi, la gestione di fenomeni di guida automatizzata e di trasporto digitale. In particolare, ci si propone

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760165

di analizzare la regolamentazione relativa alla sperimentazione su strada pubblica dei veicoli a guida autonoma nel contesto italiano, alla luce del c.d. Decreto *Smart Roads* e dei connessi problemi di *cybersecurity,* soffermandosi, in particolare, sulla vigilanza del funzionamento del sistema automatico.

In secondo luogo, l'indagine sarà rivolta a considerare il connubio tra sicurezza individuale e appalti per l'innovazione, nelle forme del partenariato per l'innovazione e dei contratti di ricerca e sviluppo per l'approdo a soluzioni di trasporto automatizzato ed eco-sostenibile e la tutela degli eco-sistemi.

In tale prospettiva, occorre considerare l'intreccio tra tecnologie informatiche, *software* applicativi e *start up* promotrici di processi di accertamento delle violazioni stradali e dell'ampliamento di soluzioni per la digitalizzazione.

Ci si propone di considerare una necessaria sinergia tra il sistema del *green procurement*[1] e la possibile progettazione di soluzioni non ancora presenti sul mercato che riducano i rischi di esternalità negative e progettino soluzioni di trasporto autonomo in applicazione del principio *security by design* (sicurezza durante la progettazione e sviluppo) che richiede competenza degli attori coinvolti in materia di *cybersecurity*.

Infine, aspetto centrale e connesso agli aspetti già tratteggiati, attiene alla regolamentazione dei *big data* e degli algoritmi che supportano i sistemi di mobilità sostenibile e sono in rapporto di intersezione con la riservatezza degli utenti.

In tale ambito, avrà senso indagare il diverso atteggiarsi del potere conoscitivo pubblico in relazione alle fattispecie di trasporto automatizzato e digitalizzato e alle procedure algoritmiche che ne sono alla base.

Riflettere sulla necessità di un archivio tutelato di dati assume importanza, ove si considerino le prospettive di ampliamento del fenomeno e la sua progressiva diffusione, valorizzando, così, *de iure condendo,* i poteri di organizzazione dell'ENISA e delle Autorità nazionali di Cybersicurezza.

Il *fil rouge* della trattazione pare riconducibile ai due poli fondamentali della sicurezza e della responsabilità, declinati nel settore della cybersicurezza e dell'introduzione/diffusione di modelli di mobilità intelligente nei contesti delle *smart cities* e delle politiche dei trasporti per le future generazioni.

Il tema investe le dinamiche partecipative dei privati ai processi decisori pubblici, ma involge, necessariamente, una riflessione sul ruolo dei pubblici poteri e sulle scelte in ordine alle modalità di *governance* idonee a regolare la complessità delle nuove applicazioni tecnologiche ai contesti socio-economici.

1 La connettività dei veicoli e l'integrazione, all'interno di un sistema, di migliaia di componenti generano minacce di attacchi informatici, come quelle sul controllo a distanza dei veicoli, che vanno regolamentate e affrontate con gli strumenti preventivi del *risk assessment.* La disposizione concernente le misure di sicurezza informatica nel Codice dei contratti pubblici è stata introdotta all'articolo 108, *Criteri di aggiudicazione degli appalti di lavori, servizi e forniture*, comma 4. Tale norma prevede che le stazioni appaltanti tengano sempre in considerazione gli elementi di *cybersicurezza* nell'approvvigionamento di beni e servizi informatici, in particolare quando l'impiego dei suddetti beni e servizi risulti essere connesso alla tutela degli interessi nazionali strategici.

2. Lo stato dell'arte europeo e nazionale in tema di *smart mobilities*

Priorità dell'attuale contesto ordinamentale sono, data l'emergenza ambientale, la riduzione della congestione e dell'inquinamento atmosferico; l'aumento della sicurezza dei trasporti e della sicurezza informatica, il migliore coordinamento tra interventi infrastrutturali e regolamentazione giuridica dell'impatto sociale prodotto dagli stessi.

I sistemi di trasporto intelligente, le reti informatiche, i nodi intermodali e le piattaforme di interoperabilità sono destinati ad assumere un ruolo paradigmatico, considerato che la diffusione di tali sistemi è funzionale al raggiungimento di obiettivi di matrice sociale e di politica economica.

L'implementazione di misure di sicurezza stradale è stata perseguita a livello europeo, ai fini della realizzazione di obiettivi di crescita economica e tutela della qualità della vita, come emerge dagli atti della Commissione europea, ma anche del Paramento dell'Unione e del Comitato economico e sociale europeo.

Nel Libro bianco della Commissione, l'aspetto economico viene anteposto a quello sociale[2] e un tale approccio dell'Unione trova conferma anche nella Proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 2006/22/CE per quanto riguarda le prescrizioni di applicazione e fissa norme specifiche per quanto riguarda la direttiva 96/71/CE e la direttiva 2014/67/UE sul distacco dei conducenti nel settore del trasporto su strada[3].

Anche il Parlamento europeo, in una recente risoluzione[4], "invita la Commissione ad assicurare che il mercato abbia un tempo sufficiente e realistico per adattarsi a queste misure". A livello nazionale, una prima regolamentazione del fenomeno è stata delineata dal *Decreto Smart Roads*[5] che ha contribuito a definire le *smart roads* come infrastrutture stradali per le quali è stato compiuto un processo di trasformazione digitale orientato a introdurre piattaforme di osservazione e monitoraggio del traffico, nonché modelli di elaborazione dei dati e delle informazioni, nel quadro della creazione di un ecosistema tecnologico favorevole all'interoperabilità tra infrastrutture e veicoli di nuova generazione.

2 "[i] trasporti sono fondamentali per la nostra economia e la nostra società. La mobilità svolge un ruolo vitale per il mercato interno e la qualità di vita dei cittadini che fruiscono della libertà di viaggiare. I trasporti sono funzionali alla crescita economica e dell'occupazione".

3 COM(2017) 278 final, 31 maggio 2017. Inoltre, la Commissione dedica una specifica comunicazione "per illustrare la strategia dell'UE per una diffusione coordinata dei sistemi C-ITS che permetta di evitare la frammentazione del mercato interno in questo settore e di creare sinergie tra le diverse iniziative". Comunicazione della Commissione, Una strategia europea per i sistemi di trasporto intelligenti cooperativi.

4 Parlamento europeo, risoluzione 14 novembre 2017, punto 52. Si v., inoltre, Risoluzione del Parlamento europeo del 18 maggio 2017 *sul trasporto stradale nell'Unione europea*, cit., punto E), nonché punti 1 ss. (in cui si parla di competitività) e 20 ss. (in cui si parla di norme sociali e condizioni di sicurezza).

5 Decreto ministeriale 28 febbraio 2018 attuativo delle numerose disposizioni della Legge di Bilancio 2018 che mirano all'ammodernamento e all'adeguamento tecnologico di tutta la rete stradale italiana all'insegna della *digital tansformation.*

Il processo di trasformazione digitale in fase di sperimentazione è orientato da modelli di gestione e verifica dei dati di progetto, nonché dal monitoraggio di sistemi orientati alla sicurezza strutturale degli elementi che compongono le infrastrutture stradali.

La prima normativa europea volta ad armonizzare le regole in materia di cybersicurezza tra Stati membri è stata la Direttiva NIS 1[6] con l'obiettivo di raggiungere un livello comune ed elevato di resilienza in UE e di innalzare la cooperazione tra gli Stati membri, creando un primo livello di armonizzazione in materia di sicurezza cibernetica.

Essa individua le categorie di soggetti a cui sono rivolte previsioni specifiche e, in particolare, gli operatori di servizi essenziali, caratterizzati come soggetti pubblici o privati che forniscono *utilities* e richiede che gli Stati adottino una strategia nazionale in materia di sicurezza cibernetica, volta a definire obiettivi strategici e priorità, nonché misure di regolamentazione a livello nazionale, volte ad assicurare la cooperazione internazionale e la collaborazione con l'ENISA attraverso meccanismi individuati.

La Direttiva NIS 1 impone, essenzialmente, obblighi e misure di sicurezza adeguate e proporzionate alla gestione dei rischi e alla prevenzione e minimizzazione dell'impatto degli incidenti di sicurezza, nonché misure relative alla segnalazione di incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati. Il quadro normativo delineato dalla Direttiva NIS 1 è stato, successivamente, rafforzato e aggiornato dalla Direttiva NIS 2[7] che ha progressivamente contribuito a eliminare le divergenze tra ordinamenti, rafforzando gli obblighi di *cybersecurity* e ampliando il numero di settori e soggetti coinvolti, nonché aumentando la cooperazione tra gli Stati per raggiungere maggiore uniformità di applicazione.

Tale Direttiva rafforza, sostanzialmente, gli obblighi già presenti all'interno della Direttiva NIS 1, quali, in particolare, le misure di sicurezza operative e organizzative adeguate e proporzionate per gestire i rischi dei sistemi di rete e le informazioni che tali soggetti utilizzano per la fornitura dei loro servizi e per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi.

La Direttiva NIS 2 fornisce un elenco minimo delle misure di sicurezza che devono essere implementate e, ove opportuno, viene prevista la notifica senza indebito ritardo degli incidenti significativi anche nei confronti dei destinatari dei servizi stessi.

A queste previsioni, si aggiungono le prescrizioni rivolte agli Stati membri, circa la necessità di prevedere misure di vigilanza ed esecuzione, nonché nuovi obblighi di condivisione delle informazioni sulla cybersicurezza.

Tale Direttiva, in particolare, ridetermina e amplia l'ambito di applicazione delle norme in materia di sicurezza dei dati e potenzia gli organi e le attività di super-

6 Essa è stata adottata il 6 luglio 2016 e recepita in Italia con il d.lgs. 65/2018 ed è stata, poi, abrogata con l'entrata in vigore della Direttiva NIS 2. La Direttiva NIS 1, acronimo di "*Network and Information Security*", viene adottata nel 2016.

7 La Direttiva UE 2022/2555, adottata il 14 ottobre 2022, dovrà essere recepita nella legislazione nazionale entro il 17 ottobre 2024.

visione a livello comunitario, al fine di razionalizzare i requisiti minimi di sicurezza ed estendere i concetti di gestione del rischio.

Da tale Direttiva scaturisce un sistema di ampliamento delle responsabilità, estesa non più soltanto all'azienda titolare del servizio, ma anche a tutti gli *stakeholder* che intervengono lungo la *supply chain.*

L'obiettivo del legislatore è di espandere la cultura e gli obblighi di sicurezza a tutti gli attori coinvolti, al fine di creare un clima di responsabilità condivisa.

Con riguardo alle nuove competenze professionali richieste ai lavoratori nel settore dell'industria della mobilità derivante dall'impiego maggiore di dispositivi informatici e automatizzati sempre più sofisticati è stato elaborato un quadro di raccomandazioni[8] sulle necessarie basi di un'alfabetizzazione digitale.

Il rischio legato ai dati prodotti dal ricorso alla tecnologia (sistemi di trasporto intelligente, intelligenza artificiale, veicoli automatizzati), non solo con riferimento ai *big data,* ma anche sotto altri profili[9], ha ottenuto regolamentazione, di recente, con una serie di atti delle autorità amministrative indipendenti.

In Italia, l'Autorità garante della concorrenza e del mercato, l'Autorità per le garanzie nelle comunicazioni e il Garante per la protezione dei dati personali hanno avviato[10] un'indagine conoscitiva congiunta, riguardante l'individuazione di eventuali criticità connesse all'uso dei cosiddetti *big data* e la definizione di un quadro di regole in grado di promuovere e tutelare la protezione dei dati personali[11], la

8 Si veda, sul punto, comunicazione della Commissione, *L'Europa in movimento. Un'agenda per una transizione socialmente equa*, nonché CESE su *Il ruolo dei trasporti nella realizzazione degli obiettivi di sviluppo sostenibile.* Sulla nozione di guida autonoma si vedano Battistella 2021: 953; Salerno 2019.

9 Secondo la definizione elaborata dalla Commissione europea (*Digital single market – Big Data,* disponibile alla pagina web https://ec.europa.eu/digital-single-market/en/big-data), "*[b]ig data refers to large amounts of data produced very quickly by a high number of diverse sources. Data can either be created by people or generated by machines, such as sensors gathering climate information, satellite imagery, digital pictures and videos, purchase transaction records, GPS signals, etc. It covers many sectors, from healthcare to transport and energy*". Sui *big data* in generale si veda OECD, *Data driven innovation. Big data for growth and well-being*, October 2015

10 In data 30 maggio 2017, l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali hanno avviato congiuntamente un'Indagine Conoscitiva per meglio comprendere le implicazioni per la privacy, la regolazione, la tutela del consumatore e l'antitrust, dello sviluppo dell'economia digitale e, in particolare, del fenomeno dei *Big Data.*

11 In data 13 marzo 2018 il Parlamento europeo A8-0036/18/ P8_TA – PROV(2018)0063) ha elaborato uno studio sulla *Strategia europea per i sistemi di trasporto intelligenti cooperativi*, nella quale il Parlamento europeo ha invitato la Commissione a pubblicare una proposta legislativa che garantisca condizioni di parità per l'accesso ai dati e alle risorse di bordo dei veicoli, tutelando i diritti dei consumatori e promuovendo l'innovazione e una concorrenza leale. Più in generale sul tema, si veda la comunicazione della Commissione, *Verso uno spazio comune europeo dei dati*, COM(2018) 232, pubblicata il 25 aprile 2018, la quale fornisce orientamenti sulla condivisione di dati tra imprese e tra imprese e pubblica amministrazione, oltre a quelli di cui alla comunicazione della medesima Commissione *Costruire un'economia dei dati europea*, COM (2017) 9 final del 10 gennaio 2017, sull'ubicazione dei dati e i principi guida indicati nella relazione della piattaforma per la diffusione dei sistemi di trasporto intelligenti e cooperativi. Si veda, inoltre, la Proposta di regolamento relativo a un quadro applicabile alla libera circolazione

concorrenza dei mercati dell'economia digitale, la tutela del consumatore a fronte dell'introduzione di sistemi di interoperatività tecnologica nei trasporti.

Al quadro normativo delineato dalle due citate Direttive si è aggiunta, di recente, la regolamentazione ad opera della CER, Direttiva *risk based*[12] che fornisce indicazioni sulla identificazione delle entità critiche, definendo misure minime e procedure comuni per il *reporting* e la cooperazione tra Stati. Tale direttiva fornisce indicazioni sulla identificazione delle entità critiche, definisce le misure minime per raggiungere un grado definito di resilienza e stabilisce procedure comuni per il *reporting* e la cooperazione tra Stati. Inizio modulo

3. Rischio, precauzione e prevenzione: il diritto della paura

Il tema della mobilità digitalizzata e automatizzata, così come attualmente configurata alla luce del quadro europeo e nazionale, interseca i temi fondamentali della sicurezza e della responsabilità.

La sicurezza dei sistemi informatici è da intendersi come nuova rilevante frontiera dell'esercizio del potere amministrativo con funzione di prevenzione.

La rilevanza della connessione tra benessere complessivo e sicurezza emerge dall'art. 3, co. 2 TUE che specifica che "l'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia", nonché dall'art. 4 c.2 TUE nella parte in cui precisa il necessario rispetto dell'identità nazionale e delle funzioni dello Stato nel mantenimento dell'ordine pubblico e nella tutela della sicurezza nazionale.

A differenza di un originario sistema fondato su autoritatività e prescrittività, in cui la sicurezza radicava il proprio inveramento nell'esercizio di poteri impositivi, nell'attuale ordinamento costituzionale, tuttavia, trova fondamento il principio di proporzionalità, quale strumento di modulazione dell'intervento dei pubblici poteri.

dei dati non personali, COM (2017) 495 del 13 settembre 2017 che ha l'obiettivo di rimuovere le restrizioni ingiustificate in materia di localizzazione dei dati, rafforzando la libertà delle aziende di archiviare o trattare i propri dati non personali ovunque vogliano all'interno dell'Unione.. FOTINA, *Rete senza regole, ci provano le Autorità*, in *Il Sole 24 Ore* del 26 gennaio 2018. Anche la OECD (*Technology Foresi-ght Forum 2016 on Artificial Intelligence (AI)*, 17 November 2016, consultabile alla pagina web http://www.oecd.org/internet/ieconomy/technology-foresight-forum-2016. htm) osserva come il tema della intelligenza artificiale, in particolare, sia sottovalutato da "*policymakers and the public at large*", soprattutto se si tiene conto della circostanza che "*[i]t is widely claimed that artificial intelligence technology, combined with "big data" and with computing power, will transform entire sectors of the economy and lead to in-depth societal changes*".

12 Tale nuova direttiva sulla resilienza e quindi sulla sicurezza cinetica delle infrastrutture critiche, oggi denominate entità critiche, che sostituisce la direttiva 114/08 sulla identificazione e designazione delle Infrastrutture critiche europee, è stata pubblicata a dicembre 2022 in Gazzetta Ufficiale, insieme con la Direttiva NIS 2 dedicata alla sicurezza *cyber* delle entità critiche e al regolamento DORA sulla sicurezza delle entità del settore finanziario e bancario. Le due direttive emanate all'unisono riconciliano il concetto di sicurezza fisica o cinetica, come si dice oggi, con quello della sicurezza logica o *cyber*. La NIS2 si occupa infatti della sicurezza cyber delle entità critiche e altamente critiche e la CER della loro resilienza rispetto a minacce cinetiche sia naturali che antropiche, volontarie o involontarie, ivi comprese le minacce di stampo terroristico.

L'individuazione della nozione di sicurezza diviene nodo problematico, trattandosi di una nozione sfuggente e dai confini incerti, identificata in senso positivo con la nozione di ordine pubblico interno e internazionale.

La parabola definitoria della nozione di sicurezza ha risentito, nel corso dei differenti periodi storici, delle diverse concezioni di ordine pubblico delineate e del differente peso dell'intervento dello Stato sulla sfera giuridica dei cittadini.

L'ampio concetto della funzione di polizia di sicurezza enucleato agli inizi del '900 è stato ricostruito riconducendo ad essa poteri generali di prevenzione idonei anche a comprimere la libertà personale, qualora essa sia tale da costituire minaccia per l'ordine pubblico e la sicurezza generale dei cittadini.

Le articolazioni e le esplicazioni della polizia di sicurezza erano individuabili nell'osservazione, nella prevenzione e nella repressione, al fine di impedire le violazioni dell'ordine giuridico.

Lo sviluppo dei poteri di polizia e prevenzione veniva codificato nei Testi Unici di pubblica sicurezza e introduceva un concetto di ordine pubblico dilatato, rafforzando gli strumenti finalizzati a evitare che non avvenisse "nulla di nocivo all'ordine e alla sicurezza dello Stato e delle sue parti, perché non si compiano quei fatti che, avvenuti, perturberebbero l'interesse pubblico e il privato"[13].

Anche dopo l'avvento della Costituzione si è riscontrato l'espandersi di tale tutela sul piano della sicurezza interna ed internazionale, identificando la funzione del sistema di sicurezza pubblica con una funzione negativa di conservazione dell'ordine pubblico, in termini di rimozione delle turbative prevenzione dei pericoli.

Alla base della concezione tradizionale della sicurezza, preservata tramite poteri di polizia e strumenti di prevenzione e fondata sul principio di proporzionalità, vi è il concetto di pericolo, riscontrato qualora una determinata circostanza di fatto origini una sequenza causale che, con certezza scientifica o con probabilità vicina alla certezza, condurrà alla determinazione di un danno.

Nella dogmatica successiva è stata attuata una sorta di superamento del concetto di pericolo, risultando, invece, valorizzato il concetto di tutela precauzionale a fronte dell'esistenza di rischi potenziali che attentino non solo ad aspetti materiali attinenti all'incolumità e alla sanità, ma anche ad un ordine pubblico ideale inteso in senso dinamico e comprensivo di istanze economiche e sociali[14].

Tale concezione ha preso le mosse dal concetto di rischio, inteso come danno potenziale in condizioni di incertezza causale, idoneo a determinare l'emergere di un'amministrazione del rischio, fondata sulla valorizzazione del principio di precauzione.

Nell'attuale realtà ordinamentale italiana è riscontrabile, tuttavia, una progressiva sovrapposizione tra pericolo e rischio[15], tra prevenzione e precauzione e un'evoluzione verso un sistema di tutele in cui risultino integrati i poteri di polizia intesi in senso preventivo e gli atti di *soft law*.

13 Si v. Ranelletti 1904: 216.
14 Si v. Paladin 1965: 130; Cerri 2007: 2.
15 Barone 2020: 63-68.

A tal proposito, è d'uopo rilevare come si assista a un passaggio da un diritto dell'emergenza a un diritto del rischio che tende a sfumare nella nozione di pericolo.

Si verifica una sorta di sovrapposizione tra precauzione e prevenzione. Non essendoci una certezza scientifica sul verificarsi di una determinata serie causale, si tende ad approntare degli strumenti di prevenzione che possano tener conto del bilanciamento di più fattori.

Si tende, pertanto, ad un mutamento dei modelli di regolazione. Se secondo una sfera precauzionale si tende a poteri più ampi, connotati da una regolamentazione dolce, ove si intraveda la sussistenza di una necessaria prevenzione di pericoli, si tende a spostarsi verso una regolazione più vincolante, rigida che pone parametri prescrittivi che vanno verso la sanzione e che tendano alla conformazione.

In tale contesto, alla luce della sempre maggiore rilevanza di strumenti preventivi, emerge la necessità di coordinate di regolamentazione chiare, supportate da valutazioni tecniche e temperate dal principio di proporzionalità[16].

4. La sicurezza nazionale cibernetica e la moltiplicazione dei nessi di causalità

Un'articolazione definitoria della nozione di sicurezza, così come delineata anche alla luce del nuovo complesso sistema ordinamentale, è costituita dalla *cybersicurezza*, intesa come capacità di resistere a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi in relazione ai servizi offerti o accessibili tramite tale rete o altri sistemi informativi, nonché di impedire ogni azione diretta a ostacolare il funzionamento del sistema tecnologico.[17]

In particolare l'ambito della sicurezza viene declinato, con riferimento ai sistemi di trasporto intelligente, sia come sicurezza individuale, caratterizzata da strumenti di prevenzione utilizzati al fine di realizzare gli obiettivi pertinenti alla riduzione dei fenomeni di sinistri stradali che a livello di sicurezza cibernetica, intesa con riguardo all'impedimento di attacchi informatici tali da impedire il funzionamento dei sistemi di *smart mobilities.*

La sicurezza nazionale cibernetica si configura, pertanto, come una nuova frontiera dell'esercizio del potere amministrativo con funzione di prevenzione ed è regolata dal Regolamento UE 2019/881 (*Cybersecurity act)* che prevede un inse-

16 De Nitto 2023. La Comunicazione della Commissione, *Verso uno spazio europeo della sicurezza stradale*, specifica che gli orientamenti europei per la sicurezza stradale riguardano l'orizzonte temporale fino al 2020 e "intendono definire un quadro di governance generale e obiettivi ambiziosi che servano a orientare le strategie nazionali o locali". Una posizione simile a quella espressa dalla Commissione si rinviene nella risoluzione del Parlamento europeo del 27 settembre 2011 sulla sicurezza stradale in Europa 2011-2020, punto 2, nonché più recentemente, nella prospettiva dell'economia collaborativa, nella risoluzione del Parlamento europeo del 15 giugno 2017 su un'agenda europea per l'economia collaborativa.

17 Art. 4 n. 2 direttiva NIS.

rimento di soggetti pubblici e privati nel perimetro della cybersicurezza al fine di regolamentare i fenomeni di digitalizzazione e i circuiti *blockchain*[18] estesi alle filiere produttive e al settore dei trasporti.

La diffusione di modelli di digitalizzazione nel settore della mobilità ha imposto, contestualmente all'accelerazione dei processi e alla semplificazione dei procedimenti, problemi di responsabilità. Nell'ambito dei veicoli a motore, i problemi di responsabilità già gravosi con riferimento ai nessi di causalità, da riscontrare in materia di sinistri stradali, divengono molteplici nel settore della regolamentazione per la guida autonoma e per il trasporto automatizzato e intelligente.

I problemi tradizionali di responsabilità sono affrontati, a livello di legislazione dell'Unione, da diverse fonti, come la direttiva sull'assicurazione degli autoveicoli[19] e la direttiva sulla responsabilità dei prodotti che trovano recepimento nel contesto nazionale con la delineazione dei diversi regimi di responsabilità degli Stati membri.

In ordine al risarcimento delle vittime, la direttiva sull'assicurazione degli autoveicoli prevede già il risarcimento tempestivo delle vittime degli incidenti causati dai veicoli. La diffusione di modelli di mobilità intelligente ha determinato una effettiva moltiplicazione dei nessi causali e un necessario affinamento dei paradigmi di interpretazione dei processi di causazione. All'introduzione di nuovi meccanismi di funzionamento seguono plurimi indici di rischio, per cui si verifica una proliferazione dei nessi causali e dei profili di responsabilità.

L'introduzione di gestioni *automotive* e circuiti automatizzati di regolazione dei trasporti implica, infatti, un governo degli accadimenti che possano causare un arresto delle funzionalità informatiche, una deviazione dalla processazione algoritmica preindividuata o una indebita ingerenza e/o alterazione dei *big data* inevitabilmente coinvolti nel sistema di gestione digitalizzata dei trasporti.

Nell'interruzione della logica algoritmica diviene problematica l'individuazione della serie causale effettivamente determinativa del danno, nonché dispendioso l'acclaramento eziologico, a fronte dell'effettiva moltiplicazione dei nessi.

In tale prospettiva di progressiva sovrapposizione tra rischio e pericolo e in condizioni di effettiva incertezza epistemico-scientifica emerge uno statuto della causalità fondato su modello probabilistico e controfattuale che diviene maggiormente complesso, tanto più complessa e multistrutturata si configuri la catena dei rapporti eziologici tra gli agenti. Si consideri, inoltre, come tale prospettiva di responsabilità sia contigua al tema della necessaria tutela della riservatezza e della impermeabilità dei dati sensibili inseriti nei sistemi *automotive*, la cui violazione determina profili di illegittimità suscettibili di richiedere una regolamentazione da parte delle autorità nazionali di regolazione.

18 Rubechini 2023; Giardino 2020: 123 ss.

19 Si v la recente direttiva europea 2021/2118, che dal 23 dicembre 2023 obbliga ad assicurare anche i veicoli in sosta in aree private non accessibili al pubblico. Con riferimento alla sicurezza dei prodotti si v. Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio, del 20 maggio 2019.

5. La necessità di coordinate chiare nel security by design

Dal composito quadro delineato emerge la necessità di un ruolo presente delle istituzioni pubbliche nella regolamentazione[20].

Nella prospettiva indicata, infatti, la realizzazione di obiettivi di sostenibilità e digitalizzazione passa per la definizione *ex ante* della misura della sostenibilità stessa e delle sue modalità attuative sulla base di coordinate prescrittive.

L'auspicio è nell'assunzione da parte dei pubblici poteri di iniziative di regolazione fondate su valutazioni tecniche, fondate sul principio di proporzionalità e mirate all'adozione di coordinate volte a delineare un quadro strategico dell'Unione per la sicurezza stradale per il decennio successivo al 2020 annunciato dal Consiglio, al fine di rafforzare l'ancora debole quadro giuridico dell'Unione in materia di sicurezza stradale e in materia di mobilità autonoma, consentendo la cooperazione non solo a livello intra-UE (tra Stati membri e Unione europea), ma anche a livello internazionale, sotto l'egida delle Nazioni Unite.

Si tratta, per tale via, di assoggettare l'esercizio del potere privato ad alcuni limiti inderogabili finalizzati alla prevenzione e alla neutralizzazione dei rischi di esternalità negative che, nell'epoca della transizione digitale, si sostanziano in ricadute nocive dal punto di vista economico e sociale. Ne deriva che il settore della mobilità intelligente e automatizzata diviene ambito inglobato nel perseguimento di obiettivi di transizione meta-individuali che necessitano, per poter essere realizzati, di un apparato di regole, oltre che di ampie indicazioni di principio. Pare di poter intravedere la necessaria evoluzione verso una necessaria prescrittività della normativa di settore che ridefinisca la dimensione del binomio pericolo/prevenzione e indirizzi il settore della *smart mobilities* verso una regolamentazione idonea a contemperare obiettivi di sicurezza e discernimento di responsabilità.

Bibliografia

Ammannati L. 2018, "Diritto alla mobilità e trasporto sostenibile. Intermodalità e digitalizzazione nel quadro di una politica comune dei trasporti", in *Federalismi.it* (4)1 ss.

Angelini M. 2021, "Metodologia per il cybersecurity assessment con il Framework Nazionale per la Cybersecurity e la Data Protection", in www.framesecuritynetwork.it

Barone A. 2020, "Amministrazione del rischio e intelligenza artificiale", in *European review of digital administratio & law* (1), 63 ss.

Battistella V. 2021, "Spunti di riflessione sulla conduzione dei veicoli altamente automatizzati nella circolazione stradale in una prospettiva de iure condendo", in *Dir. trasp.*, *953*.

Buoso E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli.

Caruso E. 2020, "Trasporto pubblico locale non di linea e mobilità condivisa tra continuità e discontinuità regolativa", in *Politiche e regole per la sharing mobility, Diritto e questioni pubbliche*.

20 Caruso 2020; Ammannati 2018: 1 ss.; Gaspari 2018; Quadri 2017: 39 ss.

Cerri A. 2007, "Ordine pubblico II) Diritto costituzionale. Postilla di aggiornamento" in *Enc. giur.,* XXII, 2.

De Nitto S. 2023, *La proporzionalità nel diritto amministrativo*, Torino: Giappichelli.

Gaspari F. 2018, *Smart city. Agenda urbana multilivello e nuova cittadinanza amministrativa*, Napoli: Editoraile scientifica.

Giani L. 2018, *Dal diritto dell'emergenza al diritto del rischio,* Napoli: Esi.

Giardino E. 2017, "La realizzazione delle infrastrutture di comunicazione elettronica tra poteri statali e veti locali"*,* in *Giustamm.it*.

Montessoro P.L. 2019, "Cybersecurity, conoscenza e consapevolezza come prerequisiti dell'amministrazione digitale", in *Istituzioni del* federalismo, (3), 783.

Paladin L. 1990, "Ordine pubblico, II) Diritto costituzionale", in *Enc. giur.,* XXII, 2.

Quadri S. 2017, "La governance del trasporto pubblico locale in Italia: quali prospettive?" in L. Ammannati, A. Canepa (a cura di), *Politiche per un trasporto sostenibile. Governence, multimodalità e fiscalità,* Napoli: Editoriale Scientifica, 39 ss.

Ranelletti O. 1904, "La polizia di sicurezza", in V.E. Orlando (diretto da), *Primo Trattato completo di diritto amministrativo italiano*, vol. IV, Milano, 216.

Rubechini P. 2023, *Tecnologia, blockchain e fiducia amministrativa*, Napoli: Editoriale scientifica.

Salerno F. 2020, "L'automazione nel trasporto stradale, ferroviario e multimodale", in *Riv. dir. nav.* 94 ss.

Simbula M., Giordano M.T., Oldani I. 2020, "Principi di sicurezza applicabili ai "cloud computing services": GDPR, Direttiva NIS e PSD2 a confornto (Security principles applicable to cloud computing services:comparison between GDPR, NIS Directive and PSD2)", in *Ciberspazio e Diritto* (1) 123 ss.

Giuseppe Sferrazzo

La cybersecurity nel nuovo Codice dei contratti pubblici: l'art. 108 co. 4 e le criticità per le stazioni appaltanti

Abstract: Con l'entrata in vigore del nuovo Codice dei contratti pubblici, le amministrazioni sono tenute a considerare le caratteristiche di sicurezza dei prodotti e dei servizi da acquistare come un autonomo elemento di valutazione. Quanto previsto dalla norma rischia di entrare in conflitto con la normativa sulle infrastrutture critiche e con il concetto di perimetro nazionale di sicurezza cibernetica, complicando la gestione degli appalti, soprattutto quando il contesto di utilizzo è legato alla tutela di 'interessi strategici nazionali'. Si pongono a tal fine due problemi. Il primo è che l'amministrazione interessata dovrà giustificare il collegamento con gli interessi nazionali strategici. Il secondo, legato al prima, è se le amministrazioni, in modo discrezionale e autonomo, potranno definire i criteri per differenziare le ipotesi. Ne potrebbero derivare situazioni paradossali in cui lo stesso 'bene' verrebbe qualificato in modo diverso a seconda dell'amministrazione valutatrice, motivo per cui è necessario dotare le amministrazioni capofila di strumenti culturali e informativi adeguati.

Keywords: Cybersecurity; Codice dei contratti pubblici; Componenti di cybersicurezza; Interesse nazionale strategico; Amministrazione contraente.

1. Il concetto di cybersicurezza. Delimitazione del campo d'indagine

"In un mondo sempre più digitalizzato e connesso la cybersicurezza è diventata di fondamentale importanza"[1]. Il tema legato alla cybersicurezza sebbene sia concetto ampio, pieno di sfaccettature, si lega il più delle volte a concetti di difesa e prevenzione volte alla salvaguardia di strutture organizzative informatiche pubbliche e private. Invero, il concetto nella sua complessità, non può esser limitato a sin-

1 Frase di apertura del portale sulla strategia nazionale dell'Agenzia di cybersicurezza in https://acn.gov.it/portale/strategia-nazionale-di-cybersicurezza.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760166

goli segmenti operativi, in quanto in uno "Stato digitale[2]", l'elemento *cyber* risulta correlato alla vita di tutti i giorni, compendiandosi in atti che sono centrali persino nella quotidianità del singolo cittadino, in un contesto tecnologico cangiante e destinato a innervare anche gli aspetti più impercettibili della società odierna.

In tale quadro, la sfera pubblica cade inevitabilmente al centro dell'attenzione. Lo stato dell'arte in 'salsa' digitale implica, in questa sede, un'analisi profonda del fenomeno cyber, in un contesto storico che ha evidenziato sempre più spesso l'incapacità delle amministrazioni pubbliche a dotarsi di metodi appropriati volti a creare un ambiente funzionale alle esigenze della collettività[3]. In un mondo sempre più tecnologico, solo infrastrutture digitali funzionanti ed evolute possono consentire alle amministrazioni nazionali di reggere il passo con la modernità e resistere agli attacchi cyber che imperversano sempre più tra le maglie difensive dei soggetti pubblici. A tal uopo, la difesa dei servizi e delle attività pubblicistiche vale non solo a preservare gli interessi delle singole amministrazioni al corretto raggiungimento dell'interesse pubblicistico ma deve essere strumentale, altresì, a garantire i diritti dei singoli cittadini[4]. Si tratta, in buona sostanza, di un compito cruciale che coinvolge, in via diretta, diverse istanze legate alla persona, agli interessi economici e, più in generale, ad obiettivi strategici nazionali[5].

Alla luce di quanto evidenziato, è opportuno tracciare i confini della materia.

L'elemento di resilienza cibernetica[6], in combinato disposto con quello di sicurezza cibernetica[7], si pongono fra le misure che consentono alla Repubblica italiana una difesa nazionale delle reti, dei sistemi informatici, dei servizi e delle infrastrutture tali da consentire la continuità dello svolgimento delle attività istituzionali del Paese avuto particolare riguardo ai servizi essenziali[8].

Tale presupposto non deve riguardare esclusivamente le alte sfere istituzionali del paese e i compiti più rilevanti e centrali dello Stato (inquadrabili in seno alle attività rientranti nel c.d. Perimetro di Sicurezza Nazionale Cibernetica[9]) dovendo interessare qualsiasi apparato amministrativo (perfino i più esigui) protagonisti principali ed erogatori delle prestazioni primarie presso le comunità di riferimen-

2 Torchia, 2023.

3 Piras, 2022: 426.

4 Carotti, 2020: 629.

5 Busia, 2020: 9.

6 Intendendosi con tale elemento alcuni aspetti tecnici specifici, quali la prevenzione e la risposta a minacce informatiche che possono danneggiare dati e infrastrutture informatiche.

7 Si fa riferimento ad una dimensione normativa e organizzativa di maggiore ampiezza attinente alla gestione e protezione di reti e infrastrutture, alla identificazione e rilevazione delle minacce, alla risposta e ripristino della funzionalità dei servizi e alla governance cibernetica a garanzia della efficacia e efficienza delle reti e infrastrutture.

8 Di Costanzo, 2022: 2.

9 Art. 1, co. 1, e art. 1, co. 2, lett. a), d.l. n. 105/2019, conv. l. n. 133/2019. Ci si riferisce a soggetti che svolgono un'attività essenziale per la Repubblica ovvero a soggetti, pubblici o privati, che forniscono un servizio essenziale per il mantenimento di attività civili, sociali o economiche, fondamentali per gli interessi dello Stato, in relazione a cui un possibile malfunzionamento, interruzione o impiego improprio delle proprie infrastrutture informatiche che possano comportare un pregiudizio per la sicurezza nazionale.

to. Sovente, soprattutto in tempi recenti, gli attacchi cibernetici hanno riguardato plessi amministrativi non di primo livello, bensì regionali o addirittura comunali[10], da cui si è definitivamente accertata la necessaria presenza, oltre che di figure centrali di riferimento quale l'Agenzia per la cybersicurezza nazionale (di seguito ACN), da un lato, di professionisti all'interno degli apparati dei vari enti statali e, dall'altro, di sistemi, beni e servizi capaci di proteggere gli enti locali o le amministrazioni anche meno conosciute ma che costituiscono parte centrale nella tutela e garanzia dei diritti dei cittadini[11].

Sebbene il tema presenti notevoli complessità, la precisazione si è resa necessaria per chiarire su quale profilo del più ampio tema sulla cybersicurezza si soffermerà il testo. In questa sede, si approfondiranno gli aspetti e gli strumenti di cybersicurezza delle pubbliche amministrazioni (di seguito P.A.) in particolar modo per ciò che concerne l'elemento della sicurezza e il rapporto sussistente con le regole del *public procurement*, in fase di acquisto di beni e servizi informatici.

Nel presente contributo particolare attenzione verrà data alla disciplina contenuta nel nuovo Codice dei contratti pubblici (D.lgs. n. 36/2023). Attualmente, differenziandosi dal recente passato, le complesse attività richieste alle stazioni appaltanti esigono molto più che una semplice elencazione del prodotto o del servizio da dover valutare, in realtà, contemplando l'obbligo di apprezzamenti complessi sia in via preliminare che, soprattutto, in una fase successiva, in cui la scelta è comprensiva della "costruzione" del bando di gara e della valutazione delle offerte pervenute. La selezione dell'operatore a cui affidare la gara dovrà includere tale valutazione, in un nuovo e immanente rapporto sicurezza/qualità del servizio offerto, non più svincolabile dalla attuale e moderna realtà informatica e digitalizzata.

Nella cornice generale ora delineata, si darà ampio spazio alle criticità presentate dall'attuale normativa codicistica. In effetti, nel vaglio dei documenti di gara e nella selezione dell'offerta che assicuri gli standard di sicurezza ricercati dal bene o dal servizio informatico oggetto della commessa pubblica, si richiedono ponderazioni altamente discrezionali che non poco incidono sul criterio di selezione e sulle modalità di scelta, differenziandosi a seconda che gli elementi debbano essere solo presi in considerazione ovvero debbano essere valutati autonomamente nel caso in cui la categoria dei beni e dei servizi sia collegata agli "interessi nazionali strategici", senza dimenticare la specificità della disciplina prevista per il Perimetro di Sicurezza Nazionale Cibernetica di cui se ne approfondirà il mancato coordinamento con quanto di nuovo elaborato.

10 Fra tutti, si fa riferimento all'attacco cyber subito dalla Regione Lazio, in data 5 agosto 2021, in cui si è accertata la mancanza di preparazione tra i dipendenti oltre che gli errori di progettazione circa la rete di sicurezza cyber, a fronte di un attacco di tipo "ransomware" che non ha nulla di particolarmente sofisticato e dovrebbe, al contrario, rientrare nelle capacità di gestione di un'infrastruttura critica come quella della Regione Lazio. Questo attacco e non solo, è stato uno dei casi emblematici che ha condotto, da lì a poco, alla creazione dell'Agenzia nazionale per la cybersicurezza.

11 Rossa, 2023a: 25.

2. Il quadro normativo in materia di cybersecurity: le iniziative europee e i recepimenti nazionali

Il quadro giuridico di riferimento si presenta, come definito da autorevole dottrina, "alluvionale e multilivello"[12]. La comprensione dell'assetto normativo, difatti, non è semplice in quanto ai criteri guida indicati a livello sovranazionale, si sono succeduti gli adattamenti in ambito domestico, conseguendone una struttura legislativa che concorre a complicarne la comprensione concettuale[13].

L'esigenza europea di dotarsi di un'architettura cyber sorge dagli attentati terroristici occorsi nei primi anni 2000. Da quel momento, gli iniziali sforzi si concentrarono sulla costituzione di un'Agenzia che fosse capace di coadiuvare le istituzioni europee nell'elaborazione di strategie in grado di assicurare la sicurezza delle reti e di diffondere la cultura ICT all'interno degli Stati membri e tra operatori e cittadini. Da tale necessità, difatti, sorse l'Enisa[14]. Nonostante la presenza della nuova istituzione, la coscienza europea in tema di cybersicurezza era ancora lontana dal formarsi pienamente tanto da comportare un ruolo meramente marginale del settore e, conseguentemente, dell'Agenzia stessa.

Progressivamente, la volontà di creare una regolamentazione cyber si sedimentò in capo alle Istituzioni europee, portando, dapprima, sul piano normativo, ad un primo accenno alla cybersecurity nella direttiva 2008/114/CE in tema di protezione transfrontaliera di infrastrutture critiche, per poi giungere con la direttiva 2016/1146/UE c.d. 'direttiva NIS' (*Network and Information Systems*) ad una prima e accurata regolazione del settore[15]. All'interno di quest'ultima si segnala la costituzione di un gruppo di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Team* – il c.d. CSIRT, al fine di trattare le situazioni di crisi secondo procedure predefinite, mezzi di reazione proporzionati al tipo di evento e tempistiche il più possibile contenute[16].

12 Ursi, 2023: 18.

13 Da ultimo, l'integrazione nazionale sulla normativa CER per cui si veda Cerciello, 2024: 1.

14 Reg. Ce n. 460/200437, che istituì l'Agenzia europea per la sicurezza delle reti e dell'informazione (Enisa).

15 La volontà era quella di creare uno spazio cibernetico sicuro, adottando una serie di misure, tra cui l'istituzione di un Gruppo di Cooperazione tra gli Stati membri, centri di intervento per la sicurezza informatica negli Stati membri e un'apposita autorità di controllo e una strategia programmatica in materia. Sul punto, Matassa, 2022: 635; che ne sottolinea l'importanza per aver elaborato dei criteri di identificazione comuni degli operatori di servizi essenziali europei, affidando agli Stati membri l'onere di trasmettere e aggiornare con cadenza biennale l'elenco dei soggetti pubblici e privati ricavato sulla base dei parametri indicati dall'art. 5 della Direttiva28 e dei settori indicati dall'Allegato II.

16 I compiti del CSIRT sono definiti dal D.l. 18 maggio 2018, n. 65 e dal DPCM 8 agosto 2019 art. 4. Essi includono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT.

Sempre in ambito europeo, a seguito della prima Direttiva NIS, si è intervenuti nuovamente con il regolamento Ue n. 881/2019, il c.d. Cybersecurity Act. Il testo, suddiviso in due parti, ha, da un lato, riorganizzato le funzioni dell'Enisa rafforzando la posizione dell'Agenzia quale centro nevralgico per la sicurezza dello spazio cibernetico e attore principale atto a garantire la cooperazione tra le varie figure del settore e, dall'altro, ha creato un sistema europeo per la certificazione della sicurezza informatica[17].

Rientrando in ambito nazionale, l'Italia, anche se con ritardo, ha recepito gli obblighi sovranazionali, adottando una strategia volta a dar vita ad un impianto normativo capace di costruire un'infrastruttura nazionale di cybersicurezza, attuata attraverso una serie di interventi legislativi.

Sul punto, la direttiva NIS è stata recepita con il D.lgs. 18 maggio 2018, n. 65, che ne ha definito le regole e indicato le procedure per la strutturazione di una Strategia nazionale di sicurezza cibernetica, tra cui vi rientravano le misure necessarie per la sicurezza delle reti e dei sistemi informativi italiani rivolte agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD)[18]. Successivamente, il D.l. 21 settembre 2019, n. 105, convertito dalla L. 18 novembre 2019, n. 133, istituisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)[19]

17 Sul tema e per maggiori approfondimenti Campara, 2020: 71 e ss.

18 Sica, 2022: 583.

19 Il Perimetro nazionale serve ad assicurare un livello elevato di sicurezza delle reti, dei sistemi e dei servizi informatici utilizzati da quei soggetti (pubbliche amministrazioni, enti pubblici e privati) che esercitano "una funzione essenziale dello Stato" o che prestano "un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato", seppur non rientranti nell'ambito di applicazione della citata direttiva NIS. I soggetti sono individuati in un apposito elenco, adottato con DPCM, su proposta del Comitato interministeriale per la cybersicurezza, circostanza da cui ne discende che solo le amministrazioni e gli enti rientranti all'interno del suddetto Perimetro ricevono comunicazione dell'iscrizione (art. 1, comma 2-*bis*, d.l. n. 105/2019). Come evidenziato da Previti, 2022: 73; Tra i decreti che hanno contribuito a dare attuazione alle disposizioni del d.l. n. 105/2019, si segnalano: il DPCM 30 luglio 2020, n. 131, che definisce le modalità e i criteri procedurali di individuazione dei soggetti pubblici e privati inclusi nel Perimetro nazionale (art. 1, comma 2, lett. a), nonché i criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi, dei servizi informatici da parte dei soggetti inclusi nel Perimetro (art. 1, comma 2, lett. b); il DPR 5 febbraio 2021, n. 54, che definisce le procedure e le modalità per le operazioni di valutazione spettanti al Centro di valutazione e certificazione nazionale (CVCN), attivo invero solo da luglio 2022, con riferimento alle forniture di beni e di servizi ICT richieste dai soggetti inclusi nel Perimetro (art. 1, comma 6, lett. a), b) e c); il DPCM 14 aprile 2021, n. 81, che definisce le procedure e le modalità per la notifica degli incidenti aventi impatto su reti, sistemi e servizi ICT al CSIRT Italia, nonché le misure di sicurezza relative alle reti, ai sistemi e ai servizi ICT adottate dai soggetti inclusi nel Perimetro (art 1, commi 2 e 3, lett. a) e b); il DPCM 15 giugno 2021, che individua le categorie di beni, sistemi e servizi ICT per la cui fornitura i soggetti inclusi nel Perimetro sono tenuti a seguire le procedure di valutazione spettanti al citato CVCN (art. 1, comma 6, lett. a); il DPCM 18 maggio 2022, n. 92, in vigore dal 30 luglio 2022, in materia di accreditamento degli istituendi laboratori accreditati di prova (LAP) e di raccordo tra i predetti laboratori, il suddetto CVCN e i Centri di valutazione (CV) del Ministero dell'Interno e del Ministero della Difesa (art. 1, comma 7, lett. b).

e, da ultimo, con il D.l. 14 giugno 2021, n. 82, convertito L. 4 agosto 2021, n. 109, con la quale si è istituita l'Agenzia per la cybersicurezza nazionale[20].

Nel contesto storico appena descritto, il Parlamento europeo è intervenuto nuovamente, approvando la Direttiva c.d. 'Nis2', (Dir. Ue 2022/2555, entrata in vigore il 17 gennaio 2023). Limitando l'analisi agli aspetti attinenti al presente contributo, è interessante sottolineare come la nuova direttiva prenda posizione sull'obbligo per gli Stati membri di dotarsi disponendo, tra le altre, misure strategiche riguardanti gli elementi di cybersicurezza nel settore degli appalti pubblici[21].

In ambito nazionale, la direttiva ha, dunque, imposto un cambiamento che non è tardato ad arrivare. Espressione di quanto ora evidenziato è il D.P.C.M., del 17 maggio 2022, adottato nel solco della più ampia Strategia nazionale di cybersicurezza e al fine di dotarsi di un Piano di implementazione adeguato alla protezione degli asset strategici nazionali, per il tramite di un approccio strategico orientato alla gestione del rischio di tutto il sistema Paese. In particolare, si mettono in evidenza gli aspetti concernenti la sicurezza degli approvvigionamenti e della supply chain, assumendo aspetto centrale la valorizzazione e inclusione degli elementi di sicurezza cibernetica nelle attività di procurement ICT della P.A. Il menzionato piano nel prevedere tre specifiche misure (le nn. 6,7 e 8)[22], anticipa, in grandi linee quanto effettivamente avvenuto con le innovative disposizioni contenute nel nuovo Codice dei contratti pubblici.

In altri termini, alla luce dell'importanza assunta dalla materia cyber, dimostrata anche dal susseguirsi di interventi normativi, la cybersicurezza diventa, nel quadro europeo, principio valido a regolare l'affidamento dei contratti pubblici aventi ad oggetto soluzioni tecnologiche per la P.A.[23].

20 Per un approfondimento sulla lunga scia normativa, Previti, 2022: 68 e ss.

21 In particolare, il secondo paragrafo dell'art. 7, nell'ambito della strategia nazionale per la cibersicurezza, "gli Stati membri adottano in particolare misure strategiche riguardanti: a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi; b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source".

22 Piano di implementazione Strategia nazionale di cybersicurezza 2022-2026: Misura n. 6: Introdurre norme giuridiche che valorizzino l'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della Pubblica Amministrazione, fornendo indicazioni sia a quest'ultima che agli operatori di mercato per garantire che i beni e i servizi informatici, acquistati dai soggetti pubblici nell'ambito di gare d'appalto o di specifici accordi quadro, rispondano ad adeguati livelli di cybersicurezza. Ciò, compatibilmente con la celere definizione delle relative procedure di aggiudicazione. Misura n. 7: Promuovere la realizzazione, a livello nazionale ed europeo, di un sistema di gare pubbliche impostato su criteri che garantiscano soluzioni di qualità sotto il profilo della cybersicurezza. Misura n. 8: Introdurre norme giuridiche volte a tutelare la catena degli approvvigionamenti relativi ad infrastrutture ICT rilevanti sotto il profilo della sicurezza nazionale.

23 Cocchi, 2024: 189.

Sebbene un primo tentativo di regolazione della materia sia stato abbozzato[24], è solo con il nuovo art. 108, co. 4, D.lgs. n. 36/2023 che si pone una definitiva rivoluzione nel settore in esame, per cui l'adeguata progettazione e selezione di prodotti e servizi di sicurezza informatica deve necessariamente passare dalla procedura di evidenza pubblica. In definitiva, la crescente centralità assunta dalla sicurezza delle infrastrutture digitali nel contesto attuale impone alle amministrazioni di dotarsi di mezzi cibernetici adatti a perseguire, un approccio integrato per ottimizzare la sicurezza delle infrastrutture critiche, combinando protezione fisica e cybersecurity, in modo da rispondere efficacemente alle nuove minacce[25].

3. La valutazione della nuova componente "sicurezza" e i concetti di "elementi di cybersicurezza" e "interessi nazionali strategici"

Le previsioni in materia di cybersicurezza adottate dal nuovo Codice dei contratti pubblici si pongono in controtendenza con quanto contenuto dalla previgente disciplina di cui al D.lgs. n. 50/2016.

In tale contesto, come noto, il legislatore è nuovamente intervenuto, innovando la materia, con il nuovo Codice dei contratti pubblici (D.lgs. n. 36/2023), introducendo due norme specifiche in materia di cybersicurezza da rinvenire negli artt. 19 co. 5 e 108 co. 4.

24 Sul punto, in attuazione dell'art. 29, co. 3, D.l. 21 marzo 2022, n. 21, l'ACN con circolare pubblicata il 21 aprile 2022, n. 4336, ha stabilito delle prime regole in materia che, anche in via indiretta, hanno coinvolto i fornitori privati di tecnologia, tenuti al rispetto di quanto previsto. La lett. c) individuava una disciplina applicativa e operativa, per cui tutte le stazioni appaltanti si dovevano adeguare a quanto descritto in un'ottica di generalizzata diffusione di 'best practice' nella strutturazione dei bandi di gara. Diversi fattori sono stati messi in risalto, su tutti l'istallazione e la successiva configurazione dei sistemi, oltre che l'impatto rivestito dai nuovi strumenti in un'ottica di continuità, compatibilità operativa con le varie infrastrutture presenti. Nella gestione del bando di gara rispetto all'installazione dei sistemi, la circolare poneva in capo alle stazioni appaltanti una necessaria valutazione di elementi attinenti a tutte le fasi della gestione del rischio. In altri termini, si suggeriva alle P.A., di optare per servizi e prodotti che fossero testati in una fase preliminare in modo da valutarne la loro operatività e considerarli in virtù di scelte tecnologiche che ne migliorassero le risposte in uno scenario di rischio cyber elevato, senza dimenticare i processi di controllo e manutenzione volti ad eliminare le eventuali criticità sorte. Sebbene le rilevanti novità portate dalla circolare fossero a tutti gli effetti applicabili alle stazioni appaltanti, la natura giuridica della circolare, non comportando alcun obbligo attuativo per le P.A., è stata fortemente disattesa. Nonostante ciò, permane l'utilità della stessa nell'aver creato in ambito nazionale pubblica un nuovo modo di pensare alla cybersicurezza nel settore della contrattualistica pubblica.

25 Approccio combinato che continua ancora oggi con Il recepimento delle Direttive NIS 2 e CER rappresenta un passo significativo nello sviluppo del quadro normativo nazionale in materia di cybersecurity, che porta avanti l'obiettivo dell'Unione Europea di rafforzare i livelli di sicurezza informatica degli Stati membri e garantire la resilienza dei soggetti critici e dei servizi essenziali; come evidenziato da Cerciello, 2024: 1.

Innanzitutto, è presente il nuovo art. 19 co. 5 D.lgs. n. 36/2023[26]. In un'ottica di rivoluzione del settore in commento, il legislatore ha imposto la digitalizzazione dell'intero ciclo di vita dei contratti pubblici, prescrivendo una necessaria preparazione del personale e richiedendo adeguati profili organizzativi di sicurezza. Se dal punto di vista complessivo tale soluzione brilli per innovatività, le scelte attuate sono la risultante di quanto già invero avvenuto nella prassi. Difatti, nonostante la mancanza normativa, non vi è dubbio alcuno che i soggetti operanti nel settore contrattualistico (stazioni appaltanti ed operatori economici) si fossero già dotati di una struttura interna volta ad evitare il proliferarsi di attacchi o pericoli cyber[27].

Prescindendo dall'art. 19, oggetto centrale del presente contributo è l'art. 108 co. 4 D.lgs. n. 36/2023[28], su cui è opportuno soffermarsi. La norma, assente nella prima bozza del Codice e poi successivamente introdotta[29], stabilisce che nel

26 Art. 19, co. 5, D.lgs. n. 36/2023: Le stazioni appaltanti e gli enti concedenti, nonché gli operatori economici che partecipano alle attività e ai procedimenti di cui al comma 3, adottano misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali. Le stazioni appaltanti e gli enti concedenti assicurano la formazione del personale addetto, garantendone il costante aggiornamento.

27 Rossa, 2023b, d'altra parte l'Autore in Rossa, 2024: 341 ne rileva la natura di "manifesto di politica di cybersicurezza", dato che il legislatore ha recepito quanto già messo in pratica da tempo da parte dalle pubbliche amministrazioni. Infatti, l'elemento di cybersicurezza essendo ormai divenuto cruciale per il funzionamento di ogni organizzazione, pubblica o privata, indipendentemente dalla partecipazione a procedure di gara, aveva necessariamente condotto le pubbliche amministrazioni alla ricezione delle basilari esigenze cyber in tempo di gran lunga antecedente anche rispetto a quanto contenuto dalla circolare dell'ACN.

28 Art. 108, co. 4, D.lgs. n. 36/2023: I documenti di gara stabiliscono i criteri di aggiudicazione dell'offerta, pertinenti alla natura, all'oggetto e alle caratteristiche del contratto. In particolare, l'offerta economicamente più vantaggiosa, individuata sulla base del miglior rapporto qualità/prezzo, è valutata sulla base di criteri oggettivi, quali gli aspetti qualitativi, ambientali o sociali, connessi all'oggetto dell'appalto. La stazione appaltante, al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo, valorizza gli elementi qualitativi dell'offerta e individua criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici. Nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici. Nei casi di cui al quarto periodo, quando i beni e servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento. Per i contratti ad alta intensità di manodopera, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 30 per cento.

29 Il riferimento agli elementi cyber si ritiene possa esser stato aggiunto anche in virtù delle indicazioni fornite dall'ACN in audizione parlamentare (documento disponibile al seguente link: lhttps://documenti.camera.it/leg19/documentiAcquisiti/COM08/Audizioni/leg19.com08.Audizioni.Memoria.PUBBLICO.ide-Ges.7977.15-06-2023-15-03-25.709.pdf) in cui si evidenziava che "si potrebbe, altresì, ragionare sul criterio di aggiudicazione degli appalti quando si utilizza quello dell'offerta economicamente più vantaggiosa. (…) appare di tutta importanza, quindi, che la stazione appaltante attribuisca un opportuno peso ai profili tecnico qualitativi di sicurezza cibernetica rispetto ai profili economici, non potendo rischiare che l'elemento prezzo

procedere all'aggiudicazione della commessa pubblica su attività di approvvigionamento di beni e servizi informatici, nell'utilizzare il criterio dell'offerta economicamente più vantaggiosa, le amministrazioni (stazioni appaltanti o centrali di committenza) contemplino adeguatamente gli elementi di cybersicurezza inseriti nel contesto tecnico qualitativo dell'offerta. Eccezion fatta nel caso in cui siano accertati i c.d. "interessi nazionali strategici", circostanza dalla quale discende una forte preponderanza in favore della valutazione della componente tecnica dell'offerta, a discapito della componente economica che sarà da valutare nei limiti dei dieci punti percentuali del punteggio complessivo. In altri termini, secondo quanto predisposto dalla nuova disciplina, nel caso in cui non si sia in presenza di interessi nazionali strategici, la P.A., dovrà solo valutare la presenza di tali elementi ma sarà libera, in ogni caso, di scegliere l'offerta economicamente più vantaggiosa anche se quest'ultima non presenti i migliori livelli di sicurezza dal punto di vista qualitativo-tecnico. Nel caso in cui siano presenti gli interessi nazionali strategici, invece, la maggiore qualità della componente sicurezza giustificherebbe la scelta del partecipante malgrado possa presentare un'offerta meno vantaggiosa dal punto di vista economico, in tal modo valorizzando a valle la scelta discrezionale dalla P.A.

La soluzione appena descritta si pone in linea di continuità con la scelta di eliminare il tetto massimo per il punteggio economico entro il limite del 30%[30](secondo la nota regola del c.d. 70/30[31]) alla luce della valorizzazione degli elementi qualitativi dell'offerta. In tale ottica, prevale la volontà di rimettere alle stazioni appaltanti la scelta circa l'incidenza dell'aspetto tecnico ed economico in modo da adeguare le due componenti alle effettive caratteristiche dell'appalto da assegnare[32]. In simili situazioni, si evidenzia la chiara esigenza affinché la stazione appaltante assegni opportunamente il giusto peso ai profili tecnici afferenti alla sicurezza cibernetica anche in sfavore della parte economica, in modo da valorizzare gli elementi della singola gara ed evitando, al contempo, che il prezzo diventi un fattore decisivo nella scelta, con chiara elusione di tutto l'impianto di sicurezza cibernetico[33].

sia decisivo, anche attraverso meccanismi di gara che riconoscano la necessaria attenzione che le stazioni appaltanti debbono avere per questi aspetti".

30 Art. 95, co. 10-bis, D.lgs. n. 50/2016: La stazione appaltante, al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo, valorizza gli elementi qualitativi dell'offerta e individua criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici. A tal fine la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 30 per cento.

31 Secondo quanto appreso dalla relazione illustrativa, la scelta è dipesa dall'analisi economica fatta dall'Autorità Garante della Concorrenza e del Mercato (AGCM) nel 2021, in cui se ne sono evidenziati gli elementi critici, in larga parte distorsivi delle regole presenti nel mercato (documento disponibile al seguente link: https://www.agcm.it/dotcmsdoc/relazioni-annuali/relazioneannuale2021/Relazione_annuale_2022.pdf).

32 Catarisano, 2023: 811.

33 Unica eccezione è fondata sul periodo conclusivo del quarto comma, che reintroduce nel campo dei contratti ad alta intensità di manodopera il tetto massimo del 30% al punteggio relativo all'offerta economica, derogando in via generale la nuova disciplina complessiva che non prevede alcun tetto massimo per l'offerta economica ed in particolar modo, lo stesso comma che stabilisce nel limite del 10% la valutazione in presenza di interessi strategici.

Sebbene il nuovo art. 108 co. 4 D.lgs. n. 36/2023, premi in modo convinto la componente della sicurezza, privilegiandola nel rispetto degli *asset* definiti sia dall'ordinamento italiano che dai nuovi formanti europei, il contenuto precettivo desta non poche criticità in ordine alle regole da applicare, delle definizioni da rispettare e circa l'ampia discrezionalità lasciata alle stazioni appaltanti in sede di scelta. Gli interrogativi sorgono in merito alle nozioni di "beni e servizi informatici" o di "elementi di cybersicurezza" ma soprattutto riguardo alla nuova e apparentemente contrastante definizione di "interessi nazionali strategici", che rischia di collidere con la regolamentazione di infrastrutture critiche e con il Perimetro di Sicurezza Cibernetica, rendendo ulteriormente complessa la gestione degli appalti in un settore che, come quello in esame, nasconde innumerevoli insidie.

Il riferimento è senza dubbio problematico ma nasconde solo parte delle questioni sottese alla norma in commento, laddove già non poche difficoltà sorgono, preliminarmente, in merito alla definizione di beni e servizi informatici e, in particolar modo, sul concetto di elementi di cybersicurezza.

Rispetto alla prima, si critica il campo di applicazione, incerto e quantomai ampio. Invero, è possibile reperire dalle precedenti produzioni normative delle linee guida da seguire in ordine alla perimetrazione del campo di applicazione, segnatamente dai vari Piani triennali per l'informatica nella Pubblica amministrazione. Se indubbiamente sono da considerare le strutture immateriali (da intendere come comprensivi dei dati delle P.A., insieme ai meccanismi e alle piattaforme create per offrire servizi ai cittadini) l'attenzione va focalizzata su quelle materiali. In effetti, i beni e i servizi informatici, connessi anche ai beni di connettività, sono considerati una categoria merceologica speciale[34]. All'interno di questa lista sono sicuramente da ricomprendere beni quali gli hardware, i software e soluzioni, le macchine per gli uffici amministrativi, i prodotti di networking, gli apparati di telefonia e di trasmissione dati, così come gli strumenti di elettronica, fotografia, ottica e audio/video. In altre parole, tutto ciò che attiene all'ambito informatico, seppur anche mediatamente, dovrebbe rientrare nel campo di applicazione dell'art. 108 co. 4 D.lgs. n. 36/2023.

Nonostante sussista una certa sicurezza sul punto non poche incertezze residuano nel caso in cui i beni e i servizi non siano attinenti all'ambito di applicazione ma quantunque presentino segmenti informatici o anche di connettività. In definitiva, se determinati beni dovessero appartenere ad un campo di applicazione differente (come quello stradale, ferroviario o anche sanitario) la loro esclusione comporterebbe non pochi stravolgimenti, a maggior ragione, nel caso in cui ci fosse la connessione con gli interessi nazionali strategici, discendendone un'elusione diretta della disciplina codicistica.

A dispetto di quanto appena analizzato per la categoria merceologica dei beni e servizi informatici, più incertezze sussistono in merito al concetto di elementi di cybersicurezza.

34 Di cui la legge ne impone il ricorso per l'acquisto tramite le convenzioni CONSIP o al Mercato elettronico, senza alcuna distinzione di valore e dunque anche per importi pari a 1 o 2 euro.

Se per cybersecurity ci si riferisce all'insieme di tecnologie, processi e misure di protezione progettate per ridurre il rischio di attacchi informatici, in un'ottica di riconduzione al sistema, per tecnologia di cybersicurezza si dovrebbero intendere le attività o i controlli, finanche le misure di sicurezza da disporre per proteggere l'entità interessata. Parte centrale dell'assetto di cybersicurezza sono gli elementi che, a parere di chi scrive, andrebbero ricondotti nei concetti di: reti, sistemi, dati, applicazioni e dispositivi IT (Information Technology). In sostanza, la stazione appaltante nel configurare gli elementi di cybersicurezza di un bene o servizio informatico dovrebbe includere le tecnologie, le policy e, più in generale, tutti i processi necessari per proteggere le parti più importanti dell'ecosistema IT[35].

Da ultimo, vi è il concetto di interesse nazionale strategico. La "connessione" con tale particolare interesse innesta una serie di valutazioni complesse di cui la stazione appaltante è prima protagonista affinché il "motore" cibernetico si attivi. Questa deve *in primis* effettuare una valutazione preventiva sull'oggetto della gara. Nel caso in cui il bando rientrasse nell'ambito di tutela degli interessi nazionali strategici di cui all'art. 108 co. 4 D.lgs. n. 36/2023, allora sarà necessario strutturare il capitolato individuando esattamente le parti riguardanti gli elementi di cybersicurezza[36].

Se l'opzione legislativa è volta a limitare la discrezionalità amministrativa in un settore critico come quello in oggetto (potendosi valutare il "solo" 10% del lato economico dell'offerta) la *ratio* sottesa all'intervento evidenzia la centralità assunta dal settore cyber per lo Stato[37].

La scelta è connaturata all'ampio potere discrezionale rimesso nelle mani della stazione appaltante e tale presupposto, in un contesto applicativo e definitorio quantomai indecifrabile e lacunoso, può comportare differenze in termini di scrittura del bando e determinazione dei criteri di aggiudicazione.

Tralasciando la discrezionalità nell'individuazione della connessione rimessa alla stazione appaltante, confusione e difficoltà di coordinamento sono rilevabili anche con riferimento alla creazione della nuova categoria degli interessi nazionali

35 In tali attività si ritiene siano presenti: a) Sicurezza della rete o sicurezza delle informazioni per difendersi dagli attacchi mirati a vulnerabilità e sistemi operativi, architettura di rete, server, host, punti di accesso wireless e protocolli di rete; b) sicurezza nel cloud per proteggere i dati, le applicazioni e l'infrastruttura che risiedono in cloud pubblici, privati o ibridi; c) sicurezza dell'IoT (Internet of Things) in ordine alla protezione di una moltitudine di dispositivi facenti parte di una rete IoT; d) sicurezza delle applicazioni per impedire agli aggressori di sfruttare le vulnerabilità nel software; e) gestione di identità e accessi per controllare le autorizzazioni concesse agli individui per accedere a sistemi, applicazioni e dati; f) sicurezza degli endpoint per proteggere i dispositivi connessi a Internet come laptop, server e telefoni cellulari; g) soluzioni per la sicurezza dei dati sensibili e delle risorse informative in transito o inattivi tramite metodi come crittografia e backup dei dati.

36 Monti, 2023; 2.

37 Ricotta, 2023: 102; l'autore sottolinea che "la sicurezza nel dominio cibernetico è una delle espressioni del moderno concetto di sicurezza nazionale, con il quale individuiamo quel novero di valori indispensabili sui quali si basa la stessa sopravvivenza della Repubblica come comunità di istituzioni e di cittadini e quelle indefettibili necessità ultra-individuali legate al mantenimento delle condizioni essenziali per tenere una nazione unita e proteggerne lo sviluppo".

strategici, paragonata alle altre tipologie di cui al perimetro nazionale di sicurezza cibernetica, alle infrastrutture critiche e al golden power.

Dubbi che finanche il nuovo DDL (AC1717) finalizzato ad introdurre una nuova disciplina in tema di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, è riuscito a dissipare.

4. Nuovi spunti positivi: Il nuovo DDL "cybersicurezza" e le novità legislative

Il DDL "cybersicurezza" (AC1717)[38] recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" è stato recentemente approvato anche al Senato della repubblica e, dunque, definitivamente approvato.

L'articolo 10[39] (attualmente a seguito degli emendamenti articolo 14) introduce (*rectius* aggiunge) nuovi criteri di cybersicurezza nella esaminata disciplina presente nel Codice dei contratti pubblici. In tal senso, si consente alle P.A., le società pubbliche e i soggetti privati compresi nel Perimetro di Sicurezza Cibernetica, in presenza di approvvigionamento di beni e servizi informatici, di tenere in considerazione gli elementi essenziali di cybersicurezza individuati da un DPCM da emanarsi entro 120 giorni, da parte del Presidente del Consiglio dei ministri su proposta dell'ACN.

Passando brevemente in rassegna le principali novità contenute nel testo, è necessario previamente individuare l'ambito di applicazione soggettivo per poi considerare *se* e *come* le nuove previsioni possano modificare quanto contenuto all'interno del nuovo Codice dei contratti e, in particolar modo, dell'art. 108 co. 4 D.lgs. n. 36/2023.

Per quel che concerne l'ambito di applicazione soggettivo, i soggetti individuati sono quelli indicati nell'articolo 2, comma 2, del codice dell'amministrazione digi-

38 Il testo del D.D.L 16 febbraio 2024 A.C. 1717, così come approvato dalla Camera dei deputati è consultabile su https://www.senato.it/service/PDF/PDFServer/BGT/01418571.pdf.

39 Art. 14, co. 1, D.D.L. Senato n. 1143: Con decreto del Presidente del Consiglio dei ministri, da adottare entro cento venti giorni dalla data di entrata in vigore della presente legge, su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la sicurezza della Repubblica, di cui all'articolo 5 della legge 3 agosto 2007, n. 124, nella composizione di cui all'articolo 10, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice del l'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collabo razione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

tale (D.Lgs. 82/2005) che saranno tenuti a rispettare gli elementi essenziali in fase di acquisto di beni ICT[40].

Critica per collocazione sistematica ma opportuna per quanto previsto, risulta il secondo comma dell'attuale art. 14, in cui si compendiano una serie di obblighi e facoltà in capo alle stazioni appaltanti rispetto agli elementi essenziali di cybersicurezza individuati dal comma precedente. In particolare, si consente l'esercizio di facoltà di cui agli articoli 107, comma 2, e 108, comma 10, D.Lgs. 36/2023, nell'accertarsi dell'assenza degli elementi essenziali di cybersicurezza. Trattasi segnatamente del potere dato in capo alla P.A., circa la "riserva di non aggiudicazione"[41], precisandosi che di tale facoltà la stazione appaltante può avvalersi non oltre il termine di 30 giorni dalla conclusione della valutazione delle offerte. In altri termini, la stazione appaltante nel caso in cui non rinvenga gli elementi cyber connessi all'oggetto della gara, potrà procedere alla non assegnazione all'offerente, malgrado quest'ultimo abbia presentato l'offerta economicamente più vantaggiosa.

In effetti, è chiaro il collegamento effettuato dal DDL, laddove l'art. 107 co. 2, D.Lgs. 36/2023, nel richiamare le sole materie afferenti all'ambiente, il sociale e l'ambito giuslavoristico, preclude la possibilità di applicare la disposizione nel caso in cui si vertesse in materia di cybersicurezza. Sebbene l'accenno sia apprezzabile dal punto di vista garantistico del sistema cyber, risulta poco conciliabile il quadro giuridico delineato, in cui una disposizione fuori contesto richiami una disciplina settoriale facente riferimento a determinate materie, mancando, principalmente, di logicità sul piano programmatico codicistico. Senz'altro più attinente appare il richiamo all'art. 108, co. 10, D.Lgs. 36/2023, in quanto la generale applicabilità della fattispecie ad una serie indefinita di casi (inidoneità di tutte le offerte rispetto all'oggetto del contratto) consente, senza alcuna difficoltà, l'applicazione al caso in esame[42].

Da ultimo, per quel che ci interessa, prescindendo dai richiami ridondanti fatti al testo di cui all'art. 108, co. 4 D.Lgs. 36/2023, è opportuno evidenziare l'introduzione di cui alla lett. c) dell'attuale art. 14 DDL, in cui si obbliga l'inserimento degli elementi di cybersicurezza tra i requisiti minimi dell'offerta, nel caso in cui sia utilizzato il criterio del minor prezzo[43]. L'intenzione del legislatore per tal via è quella di sottolineare l'indefettibilità delle prestazioni o del bene previste dalla *lex specialis* di gara, affermando, di pari passo, il concetto per cui a prescindere dalle modalità di selezione dell'operatore economico, ciò che non può mai manca-

40 Come indicato dal terzo comma dell'art. 14 DDL (AC1717) facendosi riferimento alle pubbliche amministrazioni, comprese le autorità di sistema portuale e le autorità amministrative indipendenti di garanzia, vigilanza e regolazione; i gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; le società a controllo pubblico, escluse le società quotate a meno che non gestiscano servizi di pubblico interesse.

41 Cancrini, Vagnucci 2023: 329.

42 Nannipieri, 2024: 4.

43 Art. 108, co. 3, D.lgs. n. 36/2023: Può essere utilizzato il criterio del minor prezzo per i servizi e le forniture con caratteristiche standardizzate o le cui condizioni sono definite dal mercato, fatta eccezione per i servizi ad alta intensità di manodopera di cui alla definizione dell'articolo 2, comma 1, lettera e), dell'allegato I.1.

re sono le suindicate condizioni di partecipazione alla procedura selettiva, come, d'altronde, evidenziato dalla stessa giurisprudenza amministrativa[44]. Il rispetto dei requisiti minimi dell'offerta, dunque, costituisce una condizione per poter partecipare alla procedura selettiva e l'eventuale non conformità ai requisiti individuati successivamente dal DPCM comporterà l'impossibilità di prendere parte alla gara con conseguente esclusione dalla stessa.

In definitiva, se da un lato, le novità legislative rafforzano, completando, la disciplina codicistica, dall'altro lato, appare senz'altro discutibile la scelta di farlo con un altro strumento legislativo correlato, appartenente ad altro settore di riferimento. Più opportunamente, si sarebbe (forse) dovuta riconoscere la parziale fallibilità della disciplina, contemplando la possibilità di un'integrazione in via diretta sulla norma del nuovo Codice[45]. In tal modo, si sarebbe consentita una migliore collocazione sistematica delle previsioni, oltre ad un supporto agli operatori del settore che, da sempre, navigano in un mare quantomai sovraffollato di regole da rispettare[46].

Non vi è dubbio, tuttavia, che l'attenzione va riposta rispetto alle definizioni circa gli elementi essenziali di cybersicurezza e gli interessi nazionali strategici, su cui è opportuno indagare con sguardo critico.

Nel nuovo assetto individuato dal DDL "cybersicurezza", non si fa più riferimento ai soli elementi di cybersicurezza ma la definizione viene contornata dal criterio dell'essenzialità. Se da un lato, tale elemento crea delle difficoltà circa l'armoniosa convivenza con quanto previsto dal Codice, dall'altro lato, l'intervento appare risolutivo rispetto al vuoto definitorio lasciato dall'art. 108, co. 4, D.lgs. n. 36/2023. In effetti, gli elementi essenziali di cybersicurezza sono definiti come "l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo". Tale ricostruzione, valorizza quanto sostenuto nel precedente paragrafo, chiarendo, nell'attesa che venga emanato il futuro DPCM, uno degli aspetti più controversi della norma[47].

Il DPCM, sebbene risolva il dubbio classificatorio, apre ad un'ulteriore questione circa il requisito dell'essenzialità degli elementi apparso per la prima volta nel DDL e alla sua eventuale distinzione rispetto a quanto contenuto nell'art. 108 co. 4 D.lgs. n. 36/2023, in cui si fa riferimento ai soli "elementi di cybersicurezza". In attesa di chiarimenti, si possono dedurre una serie di considerazioni.

Gli elementi evidenziati dal Codice rispetto a quelli essenziali presenti nel DDL potrebbero definirsi come "ordinari" o quantomeno non essenziali. Il dubbio per-

44 Cons. Stato, sez. V, 27 ottobre 2022, n. 9249; Cons. Stato sez. V, 1° dicembre 2022, n. 10577; Cons. Stato sez. V, 12 gennaio 2023, n. 423.

45 Alla luce anche del nuovo ed imminente correttivo al nuovo Codice dei contratti pubblici, in fase di pubblicazione in Gazzetta ufficiale.

46 Sul punto, Carbone, 2023: 9 e ss; che nell'analizzare il lavoro che ha portato all'introduzione del nuovo Codice dei contratti, ha definito punto focale del lavoro il lavoro di semplificazione attuato, comportante, tra le altre misure, la riduzione delle regole da rispettare da parte delle amministrazioni interessate.

47 Per un ulteriore approfondimento si v. nota 35.

mane nel caso in cui, la disciplina indicata dallo strumento legislativo in attesa di approvazione, possa essere suscettibile di applicazione se non si sia in presenza di elementi essenziali[48]. È più probabile, a parere di chi scrive, che si sia trattato di una svista dal punto di vista letterale, per cui nei casi in cui si presentino degli elementi cibernetici (anche non essenziali) connessi ad interessi nazionali strategici, dovrebbe trovare applicazione la disciplina di cui all'art. 14 del DDL cybersicurezza.

Ma se, in questo caso, il legislatore ci verrà in soccorso chiarendo nel prossimo futuro quali di questi componenti siano da inglobare nel concetto di elementi essenziali di cybersicurezza, altrettanto non avviene per il concetto di interessi nazionali strategici, su cui non pochi dilemmi sorgono.

4.1. Le evidenti criticità: I vuoti da colmare e il mancato coordinamento con le amministrazioni operanti nel Perimetro Nazionale di Sicurezza Cibernetica

In virtù di quanto delineato nei precedenti paragrafi si possono trarre alcuni spunti di riflessione.

Innanzitutto, dati i molteplici campi attuativi e la contestuale presenza di varie definizioni che ne differenziano, circoscrivendo, il campo di applicazione sui settori e le attività essenziali per lo Stato, sarebbe auspicabile una revisione, o quantomeno come fatto con gli elementi di cybersicurezza, una specifica in ordine al corretto perimetro della definizione di interessi nazionali strategici.

Invero, se il bando dovesse riguardare prodotti o servizi "connessi" alla tutela di interessi nazionali strategici, diventerebbe necessario strutturare la gara in modo da definire la sezione afferente alla cybersecurity. L'art. 108 co. 4 D.lgs. n. 36/2023, nell'affiancare gli interessi nazionali strategici ad altre categorie già presenti all'interno del nostro ordinamento quali quelle di sicurezza nazionale[49], interesse nazionale nei settori produttivi strategici[50] e attività di rilevanza strategica[51], tuttavia difetta di una nozione organica che ne delimiti il campo di applicazione.

Sebbene manchi un concetto identificativo apparentemente, come rilevato da parte della dottrina, altra nozione può venire in soccorso, ponendosi per affinità e contiguità attuativa in posizioni simili rispetto agli interessi nazionali strategici, che è quella di "funzione essenziale dello stato[52]". In particolare, si fa riferimento

48 Come sottolineato nel paragrafo 3, la disciplina cambia e non poco se si rinvengano tali elementi, connessi con gli interessi nazionali strategici, prevedendo una ponderazione tecnica in sede di valutazione dell'offerta con valutazione del solo 10% dell'offerta economica.

49 D.l. 82/2021, agli artt. 5 e 7 si fa riferimento agli "interessi nazionali nel campo della cybersicurezza", affidando all'ACN anche la funzione di promotrice delle azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche riguardo "a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore".

50 D.l. 5 dicembre 2022, n. 187, recante "misure urgenti a tutela dell'interesse nazionale nei settori produttivi strategici".

51 D.l. 15 marzo 2012, n. 21, recante "norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni".

52 Decreto del presidente del Consiglio dei ministri 30 luglio 2020, n. 131 Regolamento

all'art. 2 co. 1, lett. a), D.P.C.M. 30 luglio 2020, n. 131, secondo cui "un soggetto esercita una funzione essenziale dello Stato … laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti".

Inoltre, chiaro indice di conformità con gli interessi nazionali strategici, è l'art. 2 co. 1, lett. b), che nel delineare i servizi essenziali, contemplando attività (quali quelle necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica o di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia) rimarca il concetto per cui anche in altri settori di riferimento, se si presentino aspetti di "rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale della competitività e dello sviluppo del sistema economico nazionale", debbano essere inquadrati in un'ottica di rilevanza strategica, non distante da quanto presumibilmente prospettato dalla nuova definizione.

L'incertezza sulla comprensione concettuale degli interessi nazionali strategici desta notevoli implicazioni anche rispetto all'eventuale accesso alle gare da parte degli operatori economici. Le scelte discrezionali delle stazioni appaltanti sul *se* e *quando* ritenere sussistenti gli interessi nazionali strategici, può pregiudicare non solo la vulnerabilità complessiva dell'infrastruttura tecnologica della P.A. italiana ma anche la concorrenza nel mercato, dato che, in alcuni casi, il rispetto degli elementi cyber potrebbe configurare un requisito per accedere ai bandi di gara. In tal senso, risulta decisiva una ponderazione degli interessi in gioco, in modo da non limitare la libertà di iniziativa economica dei soggetti operanti nel comparto di riferimento, non diminuendo, al contempo, la sicurezza delle infrastrutture tecnologiche delle amministrazioni[53]. Si auspica, dunque, un chiarimento sul punto in modo che i principi del *favor partecipationis*, della trasparenza e della *par condicio*[54], vengano rispettati e conseguentemente non si complichi la buona riuscita della novella.

Sotto altro punto di vista, tale aspetto è immanentemente collegato alle pubbliche amministrazioni rientranti nel Perimetro Nazionale di Sicurezza Cibernetica (di seguito PSNC), per cui il coordinamento con la disciplina in esame risulta ancora più complicato.

in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. Così, Nannipieri, 2024; 4.

53 Cocchi, 2024: 204; il quale auspica un ruolo operativo dell'ACN, che dovrà vigilare sull'applicazione della normativa e, nel caso, applicare le sanzioni in presenza di violazioni oltre che partecipare all'implementazione del contesto regolatorio di concerto con la presidenza del Consiglio dei ministri.

54 Sul punto è la stessa direttiva 2014/24/Ue sugli appalti pubblici che all'art. 42, par. 2, della direttiva dispone che "le specifiche tecniche consentono pari accesso degli operatori economici alla procedura di aggiudicazione e non comportano la creazione di ostacoli ingiustificati all'apertura degli appalti pubblici alla concorrenza".

Il PSNC inserito nel 2019, crea un ambito entro cui impiegare norme caratterizzate da alta specializzazione in materia di cybersicurezza nei confronti di alcuni soggetti ritenuti particolarmente sensibili e la cui azione è esercitata (anche) con reti e infrastrutture digitali[55].

La disciplina delineata coinvolge tutte le pubbliche amministrazioni presenti all'interno dell'ordinamento nazionale; potendo, quindi, interessare entità pubbliche che rientrino all'interno del PSNC o, in alternativa, determinati beni, servizi e sistemi ICT destinati ad essere impiegati sulle loro reti, ricompresi dalla disciplina normativa e regolamentare di dettaglio[56].

Per quanto riguarda la disciplina del Perimetro, essa trova applicazione sotto un duplice punto di vista. In primo luogo, essa si riferisce ai soggetti esercitanti una funzione essenziale dello Stato. In secondo luogo, esse valgono per quei soggetti, di natura pubblica o privata[57], che prestano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, in relazione a cui un possibile malfunzionamento, interruzione o impiego improprio delle proprie infrastrutture informatiche si traduce in un pregiudizio alla sicurezza nazionale.

Senza onere di esaustività, in questa sede preme ricordare gli obblighi, per i soggetti rientranti nel Perimetro, di ricorrere alle procedure di aggiudicazione di beni e servizi ICT, di cui all'articolo 1 del D.L. 105/2019[58]. In tale ambito, il ruolo del

55 Si veda Chiari, Mazzetti, 2023; Cassano, Iaselli, Spangher,2023; Giupponi, 2024; Rossa, 2024 ed in particolar modo Buoso, 2023: 98 e ss.

56 Rossa, 2023a: 153.

57 Sul punto il DDL cybersicurezza porta con sé una grossa novità contemplando la presenza anche dei soggetti privati, non compresi tra quelli risultanti dal combinato disposto dell'art.10, comma 1, del DDL 1717, da un lato e, dall'altro lato, gli artt. 2 d.lgs. 82/2005 (Codice dell'amministrazione digitale) e 1, comma 2, d.lgs. 30 marzo 2001, n. 165 (T.U.P.I.), ma rientranti nel PSNC, di cui all'articolo 1, comma 2-bis, del D.L. 105/2019. Come specificato dalla relazione tecnica, trattasi dei soggetti aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione di cui all'art. 1, co. 1, e art. 1, co. 2, lett. a), D.l. n. 105/2019. In altre parole, soggetti in settori quali quello governativo, l'interno, la difesa, lo spazio e l'aerospazio, l'energia, le telecomunicazioni, l'economia e la finanza, i trasporti, i servizi digitali e le tecnologie critiche; a cui si impongono compiti di natura preventiva per ovviare ad attacchi cyber e di carattere comunicativo nei confronti delle Autorità competenti in modo da migliorare le capacità di risposta.

58 Nel sistema di approvvigionamento dei beni ICT dei soggetti inclusi nel PSNC un ruolo centrale è svolto dal Centro di valutazione e certificazione nazionale (CVCN), organismo operante presso l'Agenzia per la cybersicurezza nazionale, disciplinato dall'articolo 1 del D.L. 105/2019. Il CVCN ha il compito di valutare la sicurezza di beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del PSNC e appartenenti alle categorie individuate dal DPCM 15 giugno 2021. I soggetti rientranti nel PSNC che intendono procedere, anche tramite le centrali di committenza (su tutti Consip e i suoi accordi quadro), all'affidamento di beni ICT sono obbligati a comunicare al CVCN per le opportune verifiche, le quali possono prevedere anche specifici test software e hardware. I fornitori di beni ICT a loro volta sono tenuti ad assicurare al CVCN la collaborazione per l'effettuazione di test. Il CVCN, inoltre, contribuisce all'elaborazione delle misure di sicurezza, definisce le metodologie di verifica e test ed elabora gli schemi di certificazione cibernetica. Il Ministero dell'interno e quello della difesa utilizzano propri centri

Centro di Valutazione e Certificazione Nazionale (da qui in poi CVCN) è di primaria importanza[59]. L'ente, nell'effettuare test di sicurezza informatica e nel controllare la solidità dei profili di cybersecurity, garantisce la stabilità delle forniture, dei servizi e dei processi considerati sensibili per la sicurezza nazionale, accertandone le capacità tecniche alla prevenzione e, eventuale, risoluzione dei problemi ad essi connessi. La disciplina si presenta in modo differente rispetto a quanto disposto dall'art. 108 co. 4 D.lgs. n. 36/2023, richiedendo, data la sensibilità degli interessi in gioco, un controllo continuo da parte del CVCN, il quale esercita le proprie competenze nel termine di quarantacinque giorni dalla comunicazione delle amministrazioni per l'affidamento di beni ICT. Il parere positivo o negativo del CVCN è dirimente sul punto, in quanto le specifiche indicazioni date dall'ente devono essere recepite nella documentazione di gara della procedura, potendosi prevedere segnalazioni piuttosto significative, tra cui l'inserimento di clausole che condizionano sospensivamente o risolutamente il contratto pubblico[60].

Proprio su questo punto si riflette il mancato coordinamento con la nuova disciplina definita dal Codice dei contratti pubblici, segnatamente se si fa riferimento ad appalti che siano connessi alla tutela di interessi nazionali strategici. Il disallineamento provoca non pochi problemi, principalmente nel caso in cui l'applicazione della disciplina di cui all'articolo 1 del D.L. 105/2019, comporti il rispetto degli *standards* di cybersicurezza da criterio di aggiudicazione a requisito di partecipazione, circostanza non prevista nella disciplina codicistica. Pertanto, in un contesto in cui l'aggiudicazione dei contratti relativi al Perimetro concerne servizi quasi esclusivamente certificati, il rispetto delle norme di cybersicurezza non è semplicemente un aspetto da "premiare", ma rappresenta una condizione necessaria per partecipare alla procedura, circostanza questa apparentemente trascurata dal nuovo Codice dei contratti[61].

In definitiva, la ricostruzione ora effettuata, fa trasparire un quadro normativo in cui a risaltare è la difficoltà definitoria riguardante gli interessi nazionali strategici e il mancato coordinamento tra l'articolo 108 e la normativa nazionale riguardante il PNSC. Tali aspetti, inevitabilmente, oltre a generare dubbi e incertezze in sede applicativa per i soggetti partecipanti nel settore di riferimento, ostacola

di valutazione in luogo del centro nazionale. Per ulteriori approfondimenti sul punto si veda Rossa, 2023a e 2024.

59 Per un approfondimento sull'ente e sui compiti svolti nel processo di acquisizione delle amministrazioni, Bruno, 2020.

60 Come rilevato da Rossa, 2024: 349.

61 Cocchi, 2024: 197 e 198; l'autore valorizza la disciplina indicata dal secondo paragrafo dell'art. 7 della direttiva Nis II, per evidenziare il disallineamento tra le due discipline, la direttiva, infatti, nel prevedere l'ambito di applicazione della strategia nazionale per la cibersicurezza, dispone che "gli Stati membri adottano in particolare misure strategiche riguardanti: a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi; b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source".

il buon andamento delle amministrazioni, aumentando il rischio del contenzioso, in un settore che è sempre stato critico e al centro di annosi dibattiti politici, con buona pace del principio del risultato, da intendere quale vera e propria stella polare posta alla base della rivoluzione copernicana intervenuta all'interno della commessa pubblica[62].

5. Cenni conclusivi

A seguito di quanto ricostruito è opportuno soppesare i *pro* e i *contro* della riforma.

Indubbiamente, nel nuovo assetto delineato dal Codice del 2023, la materia cyber assurge a nuovo ruolo, configurandosi quale vero e proprio fattore di rilevante importanza. Tale elemento non va più considerato in correlazione all'oggetto dell'appalto ma deve essere riletto con nuova centralità, tale da poter comportare anche un cambio delle normali regole applicabili.

In effetti, l'apprezzamento dell'elemento cyber diviene essenziale, circostanza da cui scaturisce l'anteporsi di tale valutazione rispetto all'oggetto globale del contratto, in un'inversione di priorità logica e interferenziale che denota l'emersione della centralità della cybersicurezza in una realtà odierna fortemente incentrata sul *dataset.*

Rispetto ai tratti essenziali della disciplina, è chiaro che prescindendo dagli interessi nazionali strategici o meno, la stazione appaltante dovrà valutare attentamente l'oggetto della gara, tenendo comunque "in debita considerazione" la materia cyber. Tutto ciò non può che essere accolto favorevolmente, laddove l'intenzione legislativa mira a creare un "nuovo" assetto di interessi in cui risulta imprescindibile l'apporto fornito dagli appartenenti alla P.A., imponendo un onere generale per ogni stazione appaltante di conoscere e fronteggiare gli elementi di cybersecurity.

In questo aspetto risiede la prima criticità. Le amministrazioni sono capaci di valutare l'oggetto cyber insito nella gara e, eventualmente, motivare il collegamento con gli interessi nazionali strategici? Tale considerazione non è scevra di conseguenze, anche centrali, nell'applicazione del dato normativo. Senza dubbio, la più significativa permane il pericolo che ciascuna stazione appaltante decida in autonomia i criteri da seguire per mettere in risalto le gare cyber, giungendo al pa-

62 Sul punto, si richiamano le annotazioni di Nannipieri, 2024; 5; in cui si critica: "sul piano sistematico, la previsione di cui al comma 4, nella versione riformulata con una proposta emendativa approvata durante l'esame in commissione in sede referente, secondo cui "resta fermo quanto stabilito dall'articolo 1 del citato decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di beni, sistemi e servizi di information and communication technology destinati ad essere impiegati nelle reti e nei sistemi informativi nonché per l'espletamento dei servizi informatici di cui alla lettera b) del comma 2 del medesimo articolo 1". Al di là del merito della questione, risulta piuttosto sfuggente la logica di introdurre una disposizione normativa di rango primario finalizzata a "mantenere ferma" un'altra norma di pari rango, mai abrogata".

radossale risultato in cui lo stesso bene sia qualificato in modo differente a seconda dell'amministrazione valutatrice.

In tale aspetto vi è intimamente correlata la seconda criticità della materia, l'ampia discrezionalità lasciata in capo alle P.A. In un'ottica di sistema, il nuovo Codice rilancia verso nuove modalità di cura dell'interesse pubblico incoraggiando le stazioni appaltanti ad utilizzare lo spazio discrezionale a loro riservato, in particolar modo nello sviluppo di un modo di agire che interessi il potere di tipo "tecnico"[63]. In questo senso, sembrano assumere rilievo nuovi interessi di tipo economico, sociale ma anche commerciale che, già perseguiti dall'ordinamento, si realizzano compiutamente all'interno del nuovo Codice, anche per il tramite dei principi generali, attraverso cui si riconosce nuovo e ampio spazio decisionale in capo alle autorità pubbliche[64].

Sennonché, la discrezionalità implica delle scelte, scelte che, a loro volta, richiedono un'ampia preparazione e conoscenza della materia. La P.A. deve essere in grado di motivare le valutazioni effettuate, dovendosi spingere persino a definire quando il bando debba essere connesso con gli interessi nazionali strategici. Lampante ne è la conseguenza: servono delle competenze scientifiche atte a padroneggiare il settore della cybersecurity, in un momento storico in cui non è certo che i profili professionali postulati siano disponibili in numero adeguato a tutte le stazioni appaltanti[65].

Se dal punto di vista organizzativo il legislatore si è messo in moto attraverso lo "slogan" contenuto nell'art. 19 D.lgs. n. 36/2023, d'altra parte serve agire su di un piano "individuale", in modo che i funzionari amministrativi "siano messi nelle reali condizioni di conoscere questa tematica attraverso un'azione pubblica di diffusione e di promozione della cultura della cybersecurity"[66].

Da ultimo, tali assunti sono da coordinare con il principio del risultato di cui all'articolo 1 D.lgs. n. 36/2023[67]. La logica del risultato amministrativo persegue

63 Ramajoli, 2023: 47.

64 Macchia, 2024: 31.

65 Già sostenuto in tempi non sospetti da Giannini, 1979; in cui si dedicava ampio risalto al personale ed in particolar modo alla sua formazione e addestramento; per un approfondimento in tempi più recenti a seguito delle problematiche odierne, in un'ottica sistemica rispetto a quanto dettato nel PNRR, Angeletti, 2021/ 4.

66 Rossa, 2024: 353.

67 Art.1 D.lgs. n. 36/2023: 1. Le stazioni appaltanti e gli enti concedenti perseguono il risultato dell'affidamento del contratto e della sua esecuzione con la massima tempestività e il migliore rapporto possibile tra qualità e prezzo, nel rispetto dei principi di legalità, trasparenza e concorrenza. 2. La concorrenza tra gli operatori economici è funzionale a conseguire il miglior risultato possibile nell'affidare ed eseguire i contratti. La trasparenza è funzionale alla massima semplicità e celerità nella corretta applicazione delle regole del presente decreto, di seguito denominato "codice" e ne assicura la piena verificabilità. 3. Il principio del risultato costituisce attuazione, nel settore dei contratti pubblici, del principio del buon andamento e dei correlati principi di efficienza, efficacia ed economicità. Esso è perseguito nell'interesse della comunità e per il raggiungimento degli obiettivi dell'Unione europea. 4. Il principio del risultato costituisce criterio prioritario per l'esercizio del potere discrezionale e per l'individuazione della regola del caso concreto.

l'obiettivo principale della valutazione dell'interesse sotteso all'*agere pubblicistico*, nel rispetto dei termini che ne scandiscono l'efficienza e la funzionalità. Al contempo, con tale principio si concede ampia autonomia alla P.A., nel raggiungimento di esigenze che nascono anche da obiettivi posti a livello europeo e che nella prassi si soppesano all'interno degli acquisti di beni e servizi, tra cui vi rientra, oggi, la cybersicurezza[68].

Il principio del risultato diviene espressione di un comando espresso volto a condizionare l'azione amministrativa verso l'elaborazione di parametri operativi ai quali adattare i casi concreti e le scelte discrezionali in essi operate[69]. In buona sostanza, l'art. 1 del nuovo Codice si fa portavoce del principio di imparzialità e buon andamento di cui all'art. 97 della Costituzione che oggi fornisce parametro concreto di sindacato dell'azione amministrativa[70]. Attraverso tale dogma, perno centrale attorno a cui ruotano gli altri principi[71], s'intende tutelare la certezza del rapporto contrattuale e il legittimo affidamento della parte privata nella stabilità del rapporto, facendo si che la solidità del primo porti ad una compattezza complessiva del mercato[72], ed in questo caso dei valori della cybersecurity e della sicurezza di tutte le amministrazioni.

In questo nuovo assetto di interessi, è necessario partire dalle certezze date dalla nuova disciplina in tema di cybersicurezza valorizzando il nuovo dato normativo e accrescendo il patrimonio culturale di tutta la P.A., credendo e investendo fortemente nella crescita individuale dei singoli funzionari formanti il "cuore" della mano pubblica. Dall'altro lato, in un contesto in cui si vuole neutralizzare la c.d. "paura di amministrare" e aumentare la *performance* dell'azione amministrativa, su un piano di nuova fiducia tra il settore pubblico e quello privato, i dubbi recati dalla nuova normativa, in particolar modo per quel che concerne i concetti, le definizioni date e il mancato coordinamento con la disciplina riguardante il PNSC, comporta un fattore di incertezza sul risultato finale della gara, in contrasto con quanto si fa portavoce il nuovo Codice.

Incoraggiare le stazioni appaltanti è fondamentale e riconoscergli il più ampio potere discrezionale consente di passare da una amministrazione riflessiva ad una amministrazione che opera nel "caso concreto". Ma ciò deve essere fatto con criterio logico, in virtù di una normativa che non lascia spazio a dubbi interpretativi che solo criticità possono comportare rispetto a quanto di buono prospettato. L'attuale disciplina in combinato con i nuovi principi del Codice consentono un'opera di bilanciamento che deve ispirare costantemente gli operatori del settore dato che solo in virtù di quest'ultimi la P.A. può assurgere a ruolo di "architetto delle scelte" tale

68 Sul risultato e sull'impiego delle risorse finanziarie, in un sistema di valutazione del rendimento attraverso indicatori di efficienza, Ursi, 2016: 229.

69 Per una visione completa sul principio del risultato, si veda Cintioli, 2023.

70 Spasiano, 2023a.

71 Segnatamente, il principio della fiducia (art. 2 D.lgs. n. 36/2023); il principio dell'accesso al mercato (art. 3 D.lgs. n. 36/2023); principi di buona fede e tutela dell'affidamento (art. 5 D.lgs. n. 36/2023).

72 Spasiano, 2023b.

da incentivarne l'indipendenza, aumentandone l'attitudine in sede decisionale[73], anche in un settore delicato come quello della cybersecurity.

Bibliografia

Angeletti S., 2021, "'Capacity training'. Formazione e capacità amministrativa delle PA nel Piano Nazionale di Ripresa e Resilienza", in *Rivista italiana di Public management*, vol. 4, n. 2.

Buoso E., 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli: 98 e ss.

Busia G. 2020, "Cybersecurity: una sfida per tutti", in Contaldo A.-Mula D. (a cura di), *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: IX e ss.

Bruno B., 2020, "Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *federalismi*, 14.

Campara F., 2020, "Il Cybersecurity Act", in Contaldo A., Mula D. (a cura di), *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: 70 e ss.

Cancrini A. e Vagnucci F., 2023 "Le procedure di scelta del contraente e la selezione delle offerte", in *Giorn. Dir. amm.*, 3: 329.

Carbone L., 2023, "La scommessa del 'codice dei contratti pubblici' e il suo futuro", in *Giustiziamministrativa.it:* 9 e ss.

Carotti B., 2020, "Sicurezza cibernetica e Stato nazione", in *giornale di diritto amministrativo*, 5: 629.

Cassano G., Iaselli M., Spangher G., 2022, "Cybersecurity: contesto normativo di riferimento a livello nazione ed europeo", in *Diritto di Internet, Digital Copyright e Data Protection*, 4.

Catarisano C., 2023, "Articolo 108 D.lgs. n. 36/2023", in L. Perfetti (a cura di) *Codice dei contratti pubblici commentato*, Milano: Wolters Kluwer-Ipsoa: 811.

Cerciello F., 2024, "Tra NIS 2 e CER: un filo comune per la cybersecurity e la sicurezza nazionale", in *Il Quotidiano Giuridico,* 1.

Cintioli F., 2023, "Il principio del risultato nel nuovo codice dei contratti pubblici", in *Giustiziamministrativa.it.*

Chiari C., Mazzetti A., 2023, "Cybersicurezza, le norme in vigore e in arrivo per i soggetti inclusi nel perimetro di sicurezza nazionale", in *Agenda digitale*.

Cocchi T., 2024, "La cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza", in *Munus – Rivista giuridica dei servizi pubblici*, 1: 179 – 200.

Di Costanzo C., 2022, "La resilienza cibernetica a partire da alcuni recenti documenti", in *Osservatorio sulle fonti*, 2: 1-3.

Giannini M. S., 1979, *Rapporto sui principali problemi della amministrazione dello Stato*, trasmesso alle Camere il 16 novembre.

73 Macchia, 2024: 30.

Giupponi T. F., 2024, "Il governo nazionale della cybersicurezza"*,* in *Quaderni Costituzionali,* 2.
Macchia M., 2024, "Il ruolo dei principi nel Codice dei contratti", in Macchia M. (a cura di) *Costruire e acquistare, Lezioni sul nuovo Codice dei contratti pubblici*, Torino: Giappichelli: 7 – 31.
Matassa M., 2023, "Una strategia nazionale a difesa del cyberspazio"*,* in *Pa persona e amministrazione Ricerche Giuridiche sull'Amministrazione e l'Economia*: 11/2: 635.
Monti A., 2023, "L'impatto del nuovo Codice degli appalti sulla cybersecurity della Pa", in *Formiche.net.*
Nannipieri L., 2024, "Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio", in *Rivista italiana di informatica e diritto*, 1: 1 – 5.
Piras P., 2022, "L'amministrazione digitale tra divari e doveri. 'Non camminare davanti a me, ma al mio fianco'", in *Pa persona e amministrazione Ricerche Giuridiche sull'Amministrazione e l'Economia,* 11/2: 426.
Previti L., 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi*: 25: 68 e ss.
Ramajoli M., 2023, "I principi generali", in Contessa C. e Del Vecchio P., (a cura di) *Codice dei contratti pubblici*, Vol. I, Napoli: Editoriale scientifica: 47.
Ricotta F. N., 2023, "Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria" in *Diritto Penale Contemporaneo*: 1: 102.
Rossa S., 2023 (a), Cybersicurezza e pubblica amministrazione, Napoli: Editoriale Scientifica.
Rossa S., 2023 (b), "Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario", in *Vergentis. Revista de Investigación de la Cátedra Internacional conjunta Inocencio* III, 17: 161 – 175.
Rossa S., 2024, "Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici", in *Ceridap*, 3: 1 – 15.
Sica T., 2022, "Cybersecurity e governo del rischio (Cybersecurity and risk management)", in *Corporate Governance*: 4: 583.
Spasiano M. R., 2023 (a), "Codificazione di principi e rilevanza del risultato", in C. Contessa e P. Del Vecchio, (a cura di) *Codice dei contratti pubblici*, Vol. I, Napoli: Editoriale scientifica: 49-78.
Spasiano M. R., 2023 (b), "Principi e discrezionalità nel nuovo codice dei contratti pubblici: i primi tentativi di perimetrazione del sindacato", in *Federalismi.it*, 24: 222-239.
Torchia L., 2023, *Lo Stato digitale. Una Introduzione,* Bologna: Il Mulino.
Ursi R., 2016, *Le stagioni dell'efficienza. I paradigmi giuridici della buona amministrazione,* Santarcangelo di Romagna: 229.
Ursi R., 2023, "La sicurezza cibernetica come funzione pubblica", in *La sicurezza nel cyberspazio*, a cura di Ursi R., Milano: Franco Angeli.

Simona Terracciano

La dimensione collaborativa tra soggetti pubblici e tra soggetti pubblici e privati nel contesto della cybersicurezza

Abstract: Considering the increase in hostile cyber activities targeting the digital infrastructures of public entities, it is necessary and urgent to establish an institutional framework capable of intercepting cyber threats preventively and intervening effectively to prevent or mitigate the damage from cybersecurity incidents and cyberattacks that affect fundamental public and private interests and the regular provision of public services. In this regard, the contribution analyzes some aspects of the collaboration between public entities and between public and private entities in the field of cybersecurity, focusing on recent regulatory interventions in the Italian legal system to verify if and how the Italian legislator intends to promote collaboration both in organizational and procedural terms, and through a fruitful collaboration with private entities in the procurement of ICT goods and services by public administrations.

Keywords: Cybersecurity, Cultura cyber, Cyber resilience, Collaborazione, Sanzioni.

1. Il contesto di riferimento: tra attività ostili nello spazio cibernetico, vulnerabilità delle istituzioni pubbliche e salvaguardia di interessi pubblici e privati

La Relazione annuale 2023 sulla politica d'informazione per la sicurezza, presentata al Parlamento dal Sistema di informazione per la sicurezza della Repubblica, rileva che le attività ostili nello spazio cibernetico nazionale interessano in modo crescente (e prevalente rispetto ai target privati) le infrastrutture digitali dei soggetti pubblici e, in particolare, quelle riferibili alle Amministrazioni centrali dello Stato e agli Istituti e Agenzie Nazionali[1].

1 In particolare, dalla Relazione Annuale 2023 sulla politica dell'informazione per la sicurezza (del 24 febbraio 2024) emerge che le operazioni cibernetiche condotte in danno al nostro paese hanno coinvolto, nel 2022, per il 56% target privati e per il 43% target pubblici,

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760167

In particolare, l'Agenzia per la cybersicurezza nazionale (ACN), nel corso del 2023[2], ha gestito 422 eventi cyber[3] ai danni di istituzioni pubbliche nazionali, in sensibile aumento rispetto ai 160 del 2022 e, di questi eventi, 85 sono stati classificati come incidenti[4] (nel 2022 furono 57), generando un malfunzionamento dei sistemi con conseguenti blocchi o rallentamenti nella erogazione dei servizi.

L'incremento delle offensive digitali nelle filiere delle infrastrutture digitali/servizi IT, dell'energia e dei trasporti impone la necessità di predisporre un apparato istituzionale in grado di intercettare, in un'ottica preventiva, le minacce cibernetiche e di intervenire in modo efficace per evitare o limitare i danni di incidenti di sicurezza informatica e di attacchi informatici che incidono su interessi fondamentali pubblici e privati[5].

Sebbene, infatti, la consapevolezza circa i rischi, soprattutto a livello statale, stia senz'altro aumentando negli ultimi anni[6], la vulnerabilità delle istituzioni pubbliche nel contesto della cybersicurezza rimane elevata[7] in ragione, oltre di aspetti più strettamente tecnici legati alle infrastrutture e ai sistemi, anche della mancanza di adeguate competenze specifiche all'interno delle amministrazioni[8] nonché, in generale, di una insufficiente cultura della sicurezza cyber[9]. Cultura, peraltro, che

mentre nel 2023, per il 40% target privati e per il 40% target pubblici. Nell'ambito dei target pubblici, il 65% sono Amministrazioni statali (62% nel 2022), il 2% sono strutture sanitarie pubbliche (11% nel 2022), il 22% sono Istituti e Agenzie nazionali (9% nel 2022) e il 3% sono Enti regionali, provinciali e comunali (9% nel 2022).

2 Si veda la Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale.

3 Nella Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale del 2023, per evento cyber si intende un "case con potenziale impatto su almeno un soggetto nazionale, ulteriormente analizzato e approfondito, per il quale, in base alle circostanze, il CSIRT Italia dirama alert e/o supporta, eventualmente anche in loco, i soggetti colpiti".

4 Nella definizione contenuta nella Relazione Annuale per "*incidente*" si intende "un evento cyber con impatto su confidenzialità, integrità o disponibilità delle informazioni confermato dalla vittima".

5 Se vogliamo, in larga parte già predisposto visto che l'architettura nazionale di cybersicurezza è stata strutturata dal d.l. n. 82/2021 in quattro pilastri di competenze diversificate ma complementari, che devono agire, per l'appunto, in sinergica collaborazione: il pilastro dell'informazione per la sicurezza nel dominio cyber, affidato ai Servizi; il pilastro della protezione militare, affidato al Ministero della Difesa; il pilastro della prevenzione e repressione criminale, affidato all'A.G. e alle forze di polizia di sicurezza e, infine, il pilastro della vigilanza e regolazione amministrativa affidato all'ACN.

6 Previti 2022: 67, osserva che l'accelerazione del processo di transizione digitale e le dinamiche sociali ed economico pandemiche, prima, e l'aumento esponenziale degli attacchi cibernetici riconducibili al conflitto russo-ucraino, poi, abbiano determinato un concreto manifestarsi negli ultimi anni di un reale interessamento delle istituzioni pubbliche per le rilevanti questioni problematiche poste dalla tutela della cybersicurezza.

7 Al riguardo, parlano di sistema amministrativo sotto assedio dal punto di vista digitale, Borriello & Fristachi, 2022:157

8 Rossa 2023b: 161.

9 Rossa 2023a: 220-221, "L'azione pubblica volta all'incremento delle competenze digitali e di cybersicurezza fra i dipendenti pubblici è funzionale alla diffusione di progetti e iniziative volte a promuovere una più ampia cultura della cybersicurezza, in grado di abbracciare anche

appare diffusa in modo molto diversificato tra i diversi livelli di governo territoriale laddove si consideri che le Amministrazioni locali con processi codificati di gestione degli eventi di sicurezza informatica (incidenti, allarmi di sicurezza o tentativi di attacco) sono appena il 29,2% (di cui 95,5% delle Regioni)[10].

La menzionata vulnerabilità si inserisce, d'altra parte, in un contesto di progressivo consolidamento dell'utilizzo di infrastrutture ICT e dei servizi digitali offerti sia a livello centrale sia a livello locale[11], che determina un aumento quantitativo e trasversale delle aree a rischio e fa emergere, dunque, la necessità di rafforzare la sicurezza e la resilienza informatica.

Tale esigenza risulta ancora più urgente considerando che la maggior parte degli attacchi alle istituzioni pubbliche nel 2023 ha riguardato eventi di natura *DDoS* (*Distributed Denial of Service*), ossia attacchi che mirano a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria con l'effetto di rendere indisponibili i siti e i servizi colpiti[12].

i cittadini e le imprese. Iniziative, vale a dire, dirette non tanto a coloro i quali si occupano professionalmente di cybersecurity, quanto invece a chi può imbattersi indirettamente in attacchi e incidenti cyber nell'uso quotidiani della tecnologia, da un lato sensibilizzando sui rischi esistenti e possibili e, dall'altro, educando a prevenire questi ultimi evitando di porre in essere azioni o comportamenti potenzialmente pericolosi".

10 Nel Report Pubblica Amministrazione Locale e ICT anno 2022 curato dall'Istituto Nazionale di Statistica e pubblicato il 23 febbraio 2024, si evidenzia che "Il miglioramento delle dotazioni ICT, della gestione in rete e dell'offerta online pone un accento ancor maggiore sulla necessità di valutare la sicurezza informatica delle PA locali. Il 15,1% delle PA locali ha nominato un Responsabile per la sicurezza al proprio interno (54,5% delle Regioni) o in gestione associata; invece, il 21,9% ha affidato la sicurezza ICT all'esterno, tipicamente a un fornitore di servizi (22,7% delle Regioni). Inoltre, le Amministrazioni locali con processi codificati di gestione degli eventi di sicurezza informatica (incidenti, allarmi di sicurezza o tentativi di attacco) sono appena il 29,2% (95,5% delle Regioni). Nel triennio 2020-2022 le PA locali hanno messo in campo azioni legate alla sicurezza informatica e in particolare il 79,8% ha acquistato o aggiornato software di sicurezza, il 51,2% ha preferito affidarsi a incarichi di consulenza a esperti esterni, il 36,0% ha elaborato o modificato protocolli di difesa e/o prevenzione, il 27,2% ha investito in formazione aggiuntiva al personale sulla sicurezza informatica, il 2,7% ha potuto assumere personale dedicato alla sicurezza informatica, e un'ultima parte ha indicato il disaster recovery come ulteriore area di azione".

11 Report *Pubblica amministrazione locale e ICT*, curato dall'Istituto Nazionale di Statistica, 23 febbraio 2024, in *https://www.istat.it/it/files//2024/02/Report_Ict_AP_LOCALI.pdf*, ove si legge che "Nel 2022 l'86,4% delle Regioni e il 70,4% dei Comuni consente di svolgere online l'intero iter, dall'avvio alla conclusione, di almeno un servizio pubblico locale. È in forte aumento, dal 34,3% del 2018 al 54,2%, l'utilizzo di servizi di cloud computing da parte delle PA locali. Sette amministrazioni locali su dieci non hanno una gestione codificata degli eventi di sicurezza ICT. Il 74,0% delle PA locali accede a Internet tramite connessioni veloci (almeno 30 Mbps, Megabit per secondo), mentre raddoppia (35,8%) rispetto al 2018 (17,4%) la diffusione di quelle ultraveloci (almeno 100 Mbps). Il 5,1% delle PA locali (l'81,8% delle Regioni) ha investito in intelligenza artificiale o analisi dei big data o ha pianificato di farlo nel triennio 2022-2024".

12 Cfr. Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale, pubblicata su *https://www.acn.gov.it/portale/documents/20119/446882/ACN_Relazione_2023.pdf*, par. 1.2.3, pp. 23-24.

2. La transizione digitale cyber resiliente e la (necessaria) promozione della dimensione collaborativa

Considerata l'espansione e la trasversalità del fenomeno e gli interessi pubblici e privati a rischio, risulta condivisibile l'impostazione metodologica che enfatizza come, ormai, la cybersicurezza "rileva in quanto elemento imprescindibile per il corretto funzionamento della Pubblica Amministrazione nel suo complesso, sempre più digitalizzata, senza il bisogno di relegare lo studio delle tematiche cyber a ragioni particolari quali la sicurezza dello Stato e la sicurezza pubblica"[13].

A fronte di una minaccia cyber generalizzata, in quanto indirizzata verso soggetti pubblici e privati, nonché diffusa e trasversale, dal momento che incide su molteplici aree dell'azione amministrativa e dei settori produttivi dell'economia nazionale, e considerati gli interessi fondamentali pubblici e privati suscettibili di essere pregiudicati, la garanzia di un elevato livello di sicurezza informatica e la fiducia nelle tecnologie divengono, dunque, un presupposto indispensabile per il complessivo successo della trasformazione digitale della Nazione e dell'Unione Europea.

Tale consapevolezza emerge anche dalla Strategia Nazionale Cybersicurezza 2022-2026[14], ove è previsto che la cybersicurezza "deve porsi a fondamento del processo di digitalizzazione del Paese, quale elemento imprescindibile della trasformazione digitale, anche nell'ottica di conseguire l'autonomia strategica nel settore", promuovendo, in sostanza, una *transizione digitale cyber resiliente* per il settore pubblico e per il tessuto produttivo[15].

La portata del fenomeno richiede, dunque, azioni pubbliche di prevenzione e gestione delle minacce e degli attacchi cyber che siano tempestive ed efficaci, garantendo la maggior tutela degli interessi pubblici e privati incisi.

Ebbene, tali attività e la necessità di protezione non paiono poter essere adeguatamente assicurate mediante interventi meramente settoriali e frammentari da parte di un unico soggetto isolato nel contesto nazionale e ciò in considerazione della estensione del fenomeno e delle "dimensioni mondiali della tecnica e dell'economia"[16].

13 Rossa 2023a: 28. In questo senso già Previti 2022: 82, secondo il quale "L'estensione indiscriminata, al settore della cybersicurezza, dei principi e dei caratteri che connotano l'attività amministrativa svolta dagli organismi inseriti nel Sistema (i.e., riservatezza delle comunicazioni, centralizzazione delle funzioni e unilateralità dei processi decisionali) non sembrerebbe rappresentare l'impostazione metodologica più idonea a superare le sfide per la pubblica sicurezza lanciate dalla diffusione del cyberspazio".

14 Strategia Nazionale di Cybersicurezza 2022-2026, disponibile sul sito istituzionale dell'ACN.

15 Per una analisi del quadro normativo in materia e del ruolo dell'ACN v. Chiappini 2022: 301-344; Ricotta 2023a: 356 e ss.; Ricotta 2023b: 97 e ss.

16 B. Carotti 2020: 633-634, nel commentare il d.l. 105/2019, afferma che esso "si cala sulle esigenze primarie dell'apparato, purché connesso allo svolgimento di funzioni essenziali legate agli interessi della nazione. È lo Stato-nazione ad essere protetto dal "peri-

Piuttosto, l'efficacia delle azioni appare inevitabilmente condizionata dallo sforzo collaborativo tra soggetti pubblici, anche in una dimensione multilivello, e tra soggetti pubblici e privati[17], mediante la condivisione di dati, informazioni, esperienze, conoscenze e soluzioni tecniche[18].

Lo sforzo collaborativo appare, infatti, fondamentale sia a monte, in una fase preventiva e fisiologica, per identificare e analizzare eventuali vulnerabilità e minacce e rischi in chiave previsionale e programmatica, sia a valle nella fase di gestione della crisi cibernetica, per garantire una risposta consapevole e tempestiva in base allo specifico scenario di riferimento.

Al contempo, la collaborazione tra pubblico e privato risulta nodale in un'ottica di sviluppo e innovazione, considerato che lo spazio cibernetico è costituito da prodotti e servizi ICT realizzati o erogati principalmente da soggetti privati[19].

metro", allorché si intreccia inscindibilmente con l'utilizzo di apparati quali reti, sistemi e servizi. (…) Se il decreto (…) tende verso una concezione fortemente nazionale dello Stato (…) i rischi di una lettura rigida e parcellizzata delle disposizioni divengono più elevati. In questo risiede la forte problematica che l'intervento solleva, laddove occorrerebbe un approccio maggiormente aperto, favorendo una lettura più moderna – in linea con quanto la giuspubblicistica ha insegnato ampiamente da decenni. Lo Stato, nel settore in esame, può essere tutelato benissimo anche in una dimensione più collaborativa, che è proprio quella richiesta dalla disciplina europea, secondo un disegno attuale, che sappia coniugare l'offerta di garanzie alla cittadinanza ai tempi e alle dimensioni mondiali della tecnica e dell'economia".

17 La collaborazione tra pubblico e privato quale dinamica che permea il procedimento amministrativo e la ricostruzione del procedimento amministrativo come rapporto giuridico collaborativo è stata messa in luce da autorevoli studiosi. Di recente, anche per la corposa bibliografia, si rimanda agli scritti di Chirulli 2023: 399-411; Spasiano 2021: 25-54; Bonetti 2022: 30. Parlava di "rivoluzione" Benvenuti 1994: 23, riferendosi al "capovolgimento della concezione e del posto e della funzione che spetta ai cittadini nell'ambito di uno Stato che voglia essere ispirato non più ai principii di monocrazia ma a principii di demo-crazia, i quali non possono ridursi al riconoscimento di posizioni giuridiche passive dei cittadini nei confronti dello Stato e quindi alla loro tutela, ma deve evolversi nel senso del riconoscimento di posizioni giuridiche attive nell'ambito delle funzioni, ciò che va sotto il nome di partecipazione" e di "partecipazione come libertà dei post-moderni" riferendosi al superamento "del momento tradizionale della democrazia ottocentesca basata sul riconoscimento della libertà del singolo e sulla loto protezione e, si apre al riconoscimento della libertà attiva fatta di partecipazione, e cioè della demarchia del futuro". Un contributo decisivo alla valorizzazione della partecipazione procedimentale è da attribuire agli studi di Scoca 1990: 24 e all'inquadramento dell'interesse legittimo come posizione sostanziale che dialoga con l'autorità lungo tutto il processo di formazione del procedimento. Si richiamano anche gli importanti scritti di Nigro 1980: 231 ss.; Ledda 1993: 133-172; Zito 1996: *passim* sulla natura giuridica delle pretese partecipative; Manganaro 1995; Cognetti 2000; Tarullo 2008: 354.

18 In modo approfondito nel settore della cybersicurezza, Rossa 2021: 145; Rossa 2023a: 107; Previti 2022: 82.

19 Nella Strategia Nazionale di Cybersicurezza 2022-2026, spec. p. 26, la Partnership Pubblico-Privato (PPP) è qualificata come trasversale agli obiettivi di protezione risposta e sviluppo, nonché ai fattori abilitanti (ossia formazione, promozione della cultura della sicurezza cibernetica e cooperazione).

D'altronde, la dimensione collaborativa è enfatizzata nei principali atti normativi e regolatori sovranazionali[20] e nazionali[21] in materia di cybersicurezza, nonché più in generale nell'approccio seguito dal regolatore europeo riguardo ai mercati

20 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, *Considerando* n. 3, ove si legge che "Gli ambienti TIC dei soggetti dell'Unione sono interdipendenti, utilizzano flussi di dati integrati e sono caratterizzati da una stretta collaborazione fra i loro utenti. Tale interconnessione significa che qualsiasi perturbazione, anche se inizialmente limitata a un solo soggetto dell'Unione, può avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata su altri soggetti dell'Unione. Inoltre, alcuni ambienti TIC dei soggetti dell'Unione sono connessi con gli ambienti TIC degli Stati membri, e un incidente in un soggetto dell'Unione può rappresentare un rischio per la cibersicurezza degli ambienti TIC degli Stati membri e viceversa. La condivisione di informazioni specifiche su un incidente può facilitare il rilevamento di minacce informatiche o incidenti analoghi che interessano gli Stati membri". Anche la 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), evidenzia in più punti la necessità di collaborazione tra Stati membri e UE e prevede, tra l'altro, all'art. 7, par. 1, lett. e), che la Strategia nazionale cibersicurezza di ciascuno Stato membro comprenda "l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato" e, all'art. 29, gli accordi di condivisione delle informazioni sulla cibersicurezza tra soggetti inclusi e non inclusi nell'ambito di applicazione della direttiva, al fine di prevenire o rilevare gli incidenti, a riprendersi dagli stessi o ad attenuarne l'impatto e di aumentare il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di attenuazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati. Al riguardo, rileva anche il Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 e, in particolare, gli articoli da 45 a 49.

21 Si vedano il D.lgs. 18 maggio 2018, n. 65 di attuazione della Direttiva NIS, che promuove la collaborazione tra pubblico e privato (art. 6), tra soggetti pubblici come ACN, MEF e Autorità di Vigilanza e Garante Privacy (art. 7 e 9); Anche il d.l. 14 giugno 2021, n. 82, convertito in l. n. 109/2021, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", istituisce il Comitato interministeriale per la cybersicurezza attribuendogli il compito di promuovere "l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza" (art. 4, co. 1, lett. c), nonché, tra le funzioni dell'Agenzia per la cybersicurezza nazionale prevede, lo sviluppo di capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici (art. 7). Inoltre, la Strategia nazionale di cybersicurezza 2022-2026 esplicita l'approccio "*whole-of-society*" che, oltre degli attori istituzionali con competenze in materia cyber, vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza.

e ai servizi digitali (Digital Markets Act[22], Digital Services Act[23], AI Act[24])[25], che complessivamente delineano una visione strategica fondata sulla cooperazione e condivisione multilivello di informazioni e su una sinergia tra i settori pubblico, privato e la società civile[26].

3. Alcune prospettive della dimensione collaborativa nelle recenti tendenze normative: la pianificazione e la procedimentalizzazione delle attività

Le coordinate di sistema, pur sinteticamente descritte, consentono all'interprete di analizzare le *prospettive* della dimensione collaborativa nel contesto cyber alla luce delle più recenti tendenze normative, tra le quali anche la recente legge in materia di rafforzamento della cybersicurezza nazionale e di reati informativi[27], il cui rapido iter di approvazione è stato avviato con un disegno di legge presentato dal Consiglio dei Ministri il 16 febbraio 2024[28], approvato dalla Camera dei Deputati il 15 maggio 2024[29] e approvato in via definitiva dal Senato della Repubblica in data 19 giugno 2024[30].

Tra i recenti interventi stimolati dalla intensificazione e della crescente sofisticazione delle minacce informatiche nel contesto geo-politico, con particolare riferimento alla grave crisi internazionale in atto in Ucraina, è possibile ricordare una

22 Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

23 Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

24 Al riguardo, al Summit di Seoul del 21 maggio 2024, i leader di Australia, Canada, UE, Francia, Germania, Italia, Giappone, Repubblica di Corea, Repubblica di Singapore, Regno Unito e Stati Uniti d'America, hanno sancito nella Dichiarazione di Seoul per una IA sicura, innovativa e inclusiva (punto 7) "the importance of active multi-stakeholder collaboration, including governments, the private sector, academia, and civil society to cultivate safe, innovative and inclusive Al ecosystems, and the importance of cross-border and cross-disciplinary collaboration. Recognizing that all states will be affected by the benefits and risks of AI, we will actively include a wide range of international stakeholders in conversations around AI governance".

25 In merito al DSA e DMA, Bolognini, Pelino & Scialdone (a cura di) 2023; Torchia, 2023.

26 Al riguardo, Forgione 2022: 1141.

27 Legge 28 giugno 2024, n. 90, pubblicata in G.U. n. 153 del 2 luglio 2024, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".

28 Disegno di legge del 16 febbraio 2024, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (A.C. 1717), consultabile sul sito *https://www.camera.it/leg19/126?leg=19&idDocumento=1717*.

29 Al riguardo si veda per l'analisi del testo emendato a seguito dell'esame in Commissione riunite Affari Costituzionali e Giustizia della Camera, si veda il Dossier n. 257/1 del Servizio Studi del 13 maggio 2024 contenente gli elementi per l'esame in Assemblea, pubblicato al disponibile al seguente link: *https://documenti.camera.it/leg19/dossier/pdf/AC0225a.pdf*.

30 Si rimanda al Dossier n. 257/2 del Servizio Studi del Senato del 22 maggio 2024, disponibile al link: *https://www.senato.it/service/PDF/PDFServer/BGT/01418663.pdf*.

prima direttiva del 6 luglio 2023 del Presidente del Consiglio dei Ministri rivolta alle amministrazioni pubbliche di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, volta a promuovere la gestione adeguata e coordinata delle minacce informatiche degli incidenti e delle situazioni di crisi di natura cibernetica con il supporto all'ACN, mediante "la più ampia collaborazione da parte dei soggetti impattati, nel loro stesso interesse e in quello, più generale, della resilienza cibernetica del Paese".

Tale Direttiva si è tradotta nel mese di ottobre 2023, in sede di conversione del d.l. n. 105/2023, nella introduzione della lettera *n-bis)*, all'art. 7, co. 1, del d.l. n. 82/2021[31], che ha attribuito all'ACN, nell'ambito delle funzioni di prevenzione e gestione degli incidenti e degli attacchi informatici, il potere di svolgere "ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informativa o attacchi informatici" estendendo, ai soggetti inclusi nel perimetro di sicurezza nazionale[32], ai soggetti NIS[33] (operatori di servizi essenziali e fornitori di servizi digitali) e ai soggetti Tel.co[34] (ossia le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica) in caso di mancata collaborazione, le sanzioni amministrative pecuniarie e accessorie previste dall'articolo 1, commi 10 e 14, del decreto-legge "Perimetro", nonché qualificando la mancata collaborazione come causa di responsabilità disciplinare e amministrativo-contabile.

A tale modifica normativa – che valorizza il momento collaborativo tra Agenzia e tutti i soggetti pubblici e privati impattati – ha fatto seguito un'ulteriore Direttiva del Presidente del Consiglio dei Ministri nel dicembre 2023 che, nel fornire gli indirizzi di attuazione e di coordinamento, prescrive l'adozione di atti di intesa tra ACN e Ministeri volti a procedimentalizzare il *modus operandi* delle parti in caso di attacco informatico e di misure specifiche volte nel complesso a dotare ciascun Ministero di un piano di gestione delle vulnerabilità e di reazione ove si individuino chiaramente e in via preventiva i ruoli, le responsabilità e le attività concrete per fronteggiare efficacemente l'incidente cibernetico.

Sotto un primo profilo, sembra da accogliere positivamente l'impulso alla procedimentalizzazione delle attività di gestione dei rischi e delle risposte in caso di incidenti o attacchi informatici.

Invero, la predisposizione e la adozione di tali piani in una fase fisiologica dell'azione amministrativa presuppone, a monte, un'attività di ricognizione e di analisi da parte della Amministrazione che si rivela funzionale alla comprensione dei concreti rischi potenzialmente fronteggiabili e, in generale, alla diffusione di un'effettiva cultura della cybersicurezza.

31 Cfr. Art. 7, co. 1, lett. n-bis, del d.l. n. 82/2021.

32 Art. 1, co. 2-*bis*, del d.l. n. 105/2019.

33 Art. 3, co 1, lett. g) e i), del decreto legislativo n. 65/2018.

34 Art. 40, co. 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259.

La pianificazione – nella accezione gianniniana di *attività di durata proiettata nel futuro*[35] – richiede a monte, in altri termini, una concreta presa di coscienza sul "livello di maturità della cybersicurezza"[36] da parte di ciascuna Amministrazione per garantire la adozione di misure realmente efficaci nel contesto di riferimento.

Sotto ulteriore profilo, la procedimentalizzazione consente di avere un chiaro piano di azione laddove la minaccia informatica si concretizzi, facilitando l'adozione delle azioni di risposta e, auspicabilmente, riducendo i tempi di reazione e, di conseguenza, gli eventuali effetti espansivi dell'attacco che incidono significativamente sull'Amministrazione stessa e sulle comunità di soggetti interessati.

Inoltre, il rafforzamento della dimensione collaborativa tra soggetti pubblici attraverso la procedimentalizzazione delle attività di gestione degli attacchi informatici, mostra quell'aspetto della collaborazione amministrativa intesa come il "concorso doveroso di più soggetti pubblici, tra loro distinti e separati, alla realizzazione di un fine prescritto dalla legge", ove la collaborazione non assume un carattere spontaneo, occasionale o volontaristico, ma piuttosto, essendo formalizzata, ha valore cogente, è obbligatoria e doverosa, proprio in quanto espressamente richiesta dalla legge, che impone a più soggetti pubblici di interagire all'interno di un procedimento complesso e trasversale[37].

Al riguardo, occorre rilevare che la nozione teorica di collaborazione è stata oggetto di autorevoli riflessioni, tra loro divergenti, nella scienza giuridica italiana nel corso del tempo, essendo stata qualificata, da alcuni, come espressione di tante e variate fattispecie inidonee, tuttavia, a esprimere un concetto giuridico definito[38],

35 Giannini 1983: 629, qualifica la pianificazione come "la determinazione: a) dell'ordinata temporale o di quella spaziale o di ambedue; b) dell'oggetto; c) dell'obiettivo. La pianificazione richiede sempre che si elabori un progetto, che lo si verifichi quanto alla realizzabilità, indi che si stabiliscano risorse, tempi, spazi, eventuali modi, per la realizzazione".

36 Espressione utilizzata da Longo 2024: 4.

37 Sulla *collaborazione* come "combinazione di soggetti nell'attuazione di compiti collegati, di «attività di interesse comune»; come realizzazione di un solo interesse (o fine) pubblico grazie all'apporto, necessario per legge, di più centri di potere che ne sono titolari" e sulla elaborazione della *collaborazione procedimentale* come relazione organizzativa nell'amministrazione complessa da collocare nel procedimento amministrativo e che agisce lungo tutto l'arco di determinazione della funzione e di concretizzazione dei relativi effetti, si veda D'Angelo 2022a: 190 ss. Nella stessa prospettiva, parlava di "concorso di figure che potrebbero apparire separate dalla personalità giuridica, alla produzione di una medesima attività rivolta a realizzare l'interesse dell'ordinamento" Bazoli, 1964:72. Già, Nigro 1966: 123-124 sosteneva che "Organizzazione e attività sono invece, come sappiamo, due facce della stessa moneta, due profili (due modi di essere) dello stesso sistema di istituzione e di regolazione di strumenti e di rapporti idonei a consentire il raggiungimento di determinati fini (…). [L]a collaborazione degli uffici si si esprime nella comune partecipazione all'attività amministrativa, ed a quella dell'organizzazione perché la combinazione degli uffici è solo la manifestazione della combinazione dell'azione degli stessi uffici e dei loro interessi, che è quanto soprattutto l'ordinamento vuole attuare. Il procedimento amministrativo, da una parte, è attività, o forma di attività, dall'altra ed insieme è coordinazione (azione coordinata) di uffici (cioè, di competenze, d'interessi), quindi organizzazione".

38 Si pensi alle parole di Giannini 1973: 197 che, nel trattare della "collaborazione" sostiene che essa sia un vocabolo il quale non esprime alcun concetto giuridico definito, e che

al punto, secondo altre voci, da non avere dignità teorica[39] e, da altri autori, quale concetto dotato di una propria autonomia concettuale e un significato giuridicamente rilevante e ciò anche in ragione del suo utilizzo da parte del legislatore nei testi normativi[40]. Della collaborazione è stato valorizzato, ancora, il carattere di spontaneità e l'elemento volontaristico quale espressione dell'autonomia organizzativa dei soggetti coinvolti[41], ove la collaborazione sarebbe un mero fatto, un "impegno spontaneo, volontario di soggetti diversi di concorrere, secondo le rispettive possibilità, al conseguimento di un determinato risultato"[42]. Nella molteplicità delle autorevoli ricostruzioni, appare convincente la ricostruzione della collaborazione tra autorità amministrative come "una regola normativa di azione che governa lo svolgimento delle funzioni comuni dove più soggetti, dotati di competenze distinte ma legati da relazioni organizzative procedimentali, curano un solo interesse pubblico che ad essi è cointestato; collaborando le autorità procedenti compartecipano all'esercizio del potere determinante, al potere cioè di definire il disegno legale degli effetti della funzione"[43].

In questo senso, la sicurezza e la resilienza cibernetica divengono quegli interessi propri di ciascun ente e al contempo generali, quei fini unici la cui realizzazione non può che essere condizionata dall'apporto, richiesto per legge, ai diversi soggetti pubblici che cooperano nel modo voluto dalla legge, lasciando emergere quello spirito sotteso alla collaborazione che si sostanzia nella "l'esigenza di instaurare una relazione costruttiva tra forze attive di realtà distinte"[44].

viene usato, in diritto privato, in diritto processuale, in diritto internazionale, per descrivere istituti giuridici o rapporti eterogenei, i quali richiedono poi ulteriori più precise definizioni o quantomeno determinazioni, aventi in comune un solo elemento metagiuridico, di un concorso subparitario di attività di più operatori. Tale posizione era già stata espressa dal Giannini in occasione del V Convegno di Studi di Scienza dell'Amministrazione di Varenna del 1959, in Giannini 1961: 115, ove affermava che "Io non sono riuscito a trovare né nella scienza del diritto né nella scienza dell'amministrazione un concetto di collaborazione (…) Ma per quello che io conosco attraverso i miei studi, collaborazione è un vocabolo che sta a significare semplicemente un concorso subparitario di attività (..). Qui collaborazione significa accordo di attività esecutiva, deliberativa, ecc., in cui v'è una figura soggettiva, il collaborato, che si avvale di opere di altri. Ma questo non dà luogo a ad alcuna figura giuridica, ad alcuna figura di scienza dell'amministrazione; vorrei dire che è un risultato, non è una formula organizzatoria o un rapporto. In altre parole la collaborazione, essendo una risultanza, può derivare da tante fattispecie giuridiche estremamente variate".

39 Cavallo, 2005: 368.

40 Arcidiacono 1974, 108; D'Angelo 2022b: 185.

41 Travi, 1996: 679.

42 Giovenco, 1961: 280.

43 Così, D'Angelo 2022b, al quale si rimanda per i ricchi riferimenti bibliografici. Già in D'Angelo 2022a: 203-204., l'Autore sostiene che "il contributo delle amministrazioni cooperanti si rivela decisivo per realizzare le condizioni di legittimità della funzione e degli atti cui essa mette capo. È la fattispecie precettiva che impone infatti di agire tramite quello schema di collegamento, espressione di un disegno più ampio. Ne viene che, sul piano teoretico, la collaborazione designa una regola giuridica diretta a imporre un certo assetto dell'agire amministrativo".

44 Police 2021: 72.

4. (Segue)…la legge sul rafforzamento della cybersicurezza tra collaborazione e sanzione

Nel panorama normativo più recente sul tema si inserisce anche la richiamata legge in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

L'intervento normativo si compone di 24 articoli suddivisi in due Capi – dedicati, rispettivamente alle "Disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici" (artt. 1-15) e alle "Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari" (artt. 16-24) – e si propone di rispondere alla crescente offensività delle aggressioni realizzate con mezzi telematici e informatici e alla conseguente esigenza di realizzare una più intensa tutela della sicurezza cibernetica.

Limitando l'analisi ad alcune disposizioni relative al primo capo[45], la promozione della logica collaborativa sembra emergere, anzitutto, dalla previsione che amplia soggettivamente l'obbligo di notifica di incidenti rilevanti per la cybersicurezza a soggetti ulteriori rispetto a quelli già ricompresi nel perimetro di sicurezza nazionale cibernetica[46].

Al riguardo, in reazione – con ogni probabilità – al menzionato incremento delle attività ostili a scapito di target pubblici, l'obbligo di segnalazione e notifica di incidenti[47] viene coerentemente esteso alle pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni; alle regioni e province autonome di Trento e di Bolzano; alle città metropolitane; ai comuni con popolazione superiore a 100.000 abitanti e comunque ai comuni capoluoghi di regione; alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti; alle società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane; alle aziende sanitarie locali; alle società in house degli enti menzionati, attive in alcuni specifici settori (servizi informatici, servizi di trasporto, raccolta, smaltimento e trattamento di acque reflue e gestione dei rifiuti).

45 Per una analisi dei principali temi presenti nell'originario disegno di legge, si rimanda alla sezione monografica curata da Fiornelli & Giannelli 2024.

46 Per un commento alla normativa in materia di Perimetro di sicurezza nazionale cibernetica, di cui al d.l. n. 195/2019, conv. in l. n. 133/2019, cfr. Carotti 2020: 629-641.

47 L'art. 1, co. 1, della l. n.90/2024 specifica che gli incidenti da segnalare sono quelli indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge n. 105 del 2019 che, a sua volta, richiama gli incidenti di cui all'articolo 1, comma 1, lettera h) del regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici adottato con il DPCM n. 81 del 2021 e cioè "ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici".

L'obbligo di notifica viene dunque esteso ad ulteriori soggetti pubblici e privati, oltre i confini soggettivi e oggettivi del Perimetro, individuabili attraverso l'utilizzo di una tecnica normativa redazionale tradizionale (e meno ambigua rispetto a quella utilizzata nel Perimetro)[48], mediante il rimando ad altre normative (*i.e.* elenco ISTAT) o alla indicazione di limiti numerici[49].

Tale obbligo di segnalazione e, poi, di notifica completa è soggetto a tempistiche stringenti e ciò, senz'altro, graverà le amministrazioni coinvolte di un onere organizzativo in termini di risorse umane, strumentali e finanziarie per assicurare una gestione adeguata del flusso informativo.

Sotto altro profilo, la circostanza che la reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica comporti una sanzione amministrativa pecuniaria da un minimo di 25.000 a un massimo di 125.000 euro a carico dei soggetti indicati al comma 1 dell'art. 1 della legge potrebbe essere letta come una intenzione del legislatore di dare autonoma rilevanza all'interesse *procedimentale* comunicativo e allo scambio di informazioni tra pubbliche amministrazioni in aggiunta alla tutela degli interessi *sostanziali* o *finali* rappresentati dalla sicurezza e resilienza cibernetica suscettibili di essere lesi in caso di attacco cibernetico.

In questo senso, il potere sanzionatorio, da esercitare anche nei confronti di altre amministrazioni pubbliche, pare connotarsi non tanto (o non solo) per essere espressione di una logica autoritativa e punitiva, quanto, piuttosto, per essere uno strumento a disposizione dell'amministrazione volto a sollecitare la doverosa collaborazione tra amministrazioni e a garantire l'effettività della stessa, a tutela del buon andamento dell'azione amministrativa[50].

In altri termini, così come avviene in numerosi settori dell'azione amministrativa, l'efficacia, l'effettività, l'efficienza, la tempestività, la trasparenza e il buon andamento dell'azione amministrativa, oltre ad essere fini verso i quali deve tendere l'azione amministrativa, rappresentano interessi pubblici procedimentali trasversali da preservare affinché le funzioni di amministrazione attiva, di vigilanza, di regolazione e di controllo in ciascun settore possano essere svolte in modo adeguato. Tali interessi sono concretamente perseguiti dalla pubblica amministrazione anche attraverso la sanzione amministrativa pecuniaria nella misura in cui quest'ultima è lo strumento individuato dal legislatore a garanzia della effettività degli obblighi procedimentali e collaborativi posti in capo ai soggetti pubblici e ai soggetti privati.

La stessa logica volta a promuovere l'effettività dell'obbligo di collaborazione pare permeare sia la disposizione dell'articolo 2 – ove si commina una sanzione pecuniaria nei casi di ritardata o mancata adozione degli interventi risolutivi proposti dall'ACN circa specifiche vulnerabilità alle quali risultino potenzialmente esposti le amministrazioni e gli enti pubblici e gli altri soggettivi indicati dall'ar-

48 Mette in luce le criticità definitorie del d.l. n. 105/2019, Carotti 2020: 640.

49 Un possibile profilo di criticità, a livello definitorio, potrebbe risultare dalla sovrapposizione di tali categorie con quelle di soggetti *essenziali* e *importanti* previste dalla Direttiva NIS II (art. 3 della Dir. UE 2022/2555), che dovrà essere recepita dagli Stati Membri entro il 14 ottobre 2024. Tale criticità è stata segnalata anche da Longo 2024: 3.

50 Sia consentito il richiamo a Terracciano 2023: *passim*.

ticolo, ivi inclusi i soggetti inclusi nel Perimetro, i soggetti NIS e Tel.Co– sia l'articolo 3 della legge che, nel prevedere norme di raccordo con il d.l. n. 105/2019, introduce un obbligo di segnalazione e notifica in capo ai soggetti inclusi nel Perimetro relativo a incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (di loro pertinenza), sanzionando la mancata collaborazione.

Al riguardo, la circostanza che il potere sanzionatorio amministrativo di tipo pecuniario dell'ACN sia esercitato nei confronti di altri soggetti pubblici per reagire alla mancata (doverosa) collaborazione o a comportamenti ostruzionistici sembra rendere recessivo il profilo punitivo-afflittivo dello strumento sanzionatorio e sembra, piuttosto, valorizzare la sanzione come strumento sollecitatorio e di stimolo alla collaborazione pubblica a garanzia dell'effettività delle funzioni svolte dall'Agenzia e, in generale, del buon andamento dell'azione amministrativa.

Ferma restando, dunque, la possibilità di ricavare nella dinamica obbligo-violazione-sanzione uno spazio di stimolo alla collaborazione, soprattutto quando il potere è esercitato nei confronti di un soggetto pubblico, si possono comunque segnalare alcuni aspetti critici riguardo al complessivo impianto sanzionatorio promosso dall'intervento normativo, con specifico riferimento al primo capo.

Sotto un primo profilo, la forbice edittale (tra i 25 e i 125 mila euro) per i soggetti privati appare estremamente bassa e tale da mettere in dubbio la reale capacità dissuasiva della sanzione, soprattutto laddove si consideri che in altri settori – come, ad esempio, per la violazione degli obblighi di segnalazione previsti dalla Direttiva NIS II[51] – il legislatore europeo ha previsto massimi edittali milionari o comunque parametrati ad una percentuale del totale del fatturato annuo mondiale della società.

Ulteriore profilo di rilievo appare essere quello legato alla destinazione delle sanzioni pecuniarie, in quanto l'art. 24 della legge si limita a prevedere che i proventi delle sanzioni siano destinati alle entrate dell'ACN mentre, in un'ottica di promozione virtuosa della collaborazione, sarebbe forse stato più opportuno prevedere un vincolo di destinazione dei proventi a progetti di formazione, di ricerca e sviluppo di prodotti e tecnologie, in modo da valorizzare l'azione dell'ACN quale attore istituzionalmente deputato a promuovere e supportare il processo di diffusione della cultura della cybersicurezza[52].

In linea più generale, ci si potrebbe poi domandare se la finalità di *rafforzamento della cybersicurezza* che la legge intende perseguire sia più efficacemente

51 Si veda l'art. 34 della 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 II).

52 Si condivide il pensiero di Rossa 2022a: 165, secondo cui "il fine ultimo della politica pubblica di cybersicurezza: non (sol)tanto proteggere le infrastrutture digitali, ma giungere a un contesto istituzionale di cyber resilienza in cui tutti gli attori coinvolti interagendo e collaborando fra loro in vista del raggiungimento di un obiettivo comune stabilito dallo Stato, diventino consci dei rischi cyber. Come intuibile, nel far ciò il ruolo dello Stato appare imprescindibile".

raggiungibile attraverso l'imposizione di nuove prescrizioni, obblighi informativi e di sanzioni in caso di inosservanza, ovvero mediante un cospicuo investimento, in termini di risorse umane e strumentali, per rafforzare la capacità di prevenzione e gestione degli eventi e degli attacchi cyber e la resilienza informatica complessiva.

Non pare ragionevole propendere in senso netto verso l'una o l'altra alternativa, ma piuttosto si ritiene che l'approccio autoritativo dovrebbe integrarsi con quello di promozione della collaborazione, della cultura della cybersicurezza e della acquisizione e diffusione delle competenze all'interno degli enti di ridotte dimensioni e in favore delle comunità di riferimento, al fine di evitare che la sanzione comminata a fronte dei mancati obblighi collaborativi finisca per essere la conseguenza di criticità organizzative radicate e di sistema, probabilmente non dipendenti (e, dunque, non imputabili) al singolo funzionario o alla singola amministrazione di riferimento.

In questo senso, come peraltro da tempo sostengono autorevoli voci, si condivide l'idea secondo la quale "il principale fattore di miglioramento dei rendimenti amministrativi dovrebbe proprio essere il suo capitale umano, per evitare di incorrere nell'errore di considerare il processo riformatore normativo più importante del cambiamento delle persone"[53]. La diffusione delle competenze nel settore pubblico e il cambiamento dell'ambiente culturale rispetto a queste tematiche appaiono essere, come emerge dai dati richiamati, l'oggetto di un processo lento e non ancora del tutto compreso, soprattutto nelle realtà territoriali più piccole, che, tuttavia, mal si concilia con l'urgenza regolatoria del settore generata dal frequente mutamento e dalla rapida espansione del fenomeno, nonché dalla complessità dello stesso.

Al riguardo, al fine di integrare l'approccio autoritativo e quello collaborativo, sarebbe forse stato opportuno prevedere un periodo transitorio, prima di rendere efficace l'apparato sanzionatorio previsto, durante il quale svolgere corsi di formazione specifica delle risorse umane, simulazioni ed esercitazioni per testare la capacità di preparazione e reazione ad incidenti o ad attacchi informatici, sul modello di quanto effettuato nel 2023 in favore delle amministrazioni del Nucleo per la cybersicurezza e dei soggetti pubblici inseriti nel Perimetro di sicurezza nazionale cibernetica[54].

Nell'analizzare le *prospettive* della collaborazione nel contesto della cybersicurezza, un ultimo breve cenno merita il tema della collaborazione pubblico-privato nella fase di approvvigionamento di beni e servizi ICT da parte delle istituzioni pubbliche[55].

Al riguardo, occorre notare che la prima versione del disegno di legge prevedeva di assegnare all'ACN un nuovo potere di promozione e di sviluppo di ogni iniziativa, anche di partenariato tra soggetti pubblici e privati, volta a valorizzare l'intel-

53 Ramajoli 2021: 451; Battini 2021, 11-14.

54 Nella Relazione Annuale al Parlamento 2023 dell'Agenzia per la cybersicurezza nazionale si legge che, al fine di rafforzare la capacità di gestione strategico-procedurale delle amministrazioni del Nucleo per la cybersicurezza e dei soggetti pubblici inseriti nel Perimetro di sicurezza nazionale cibernetica, sono state condotte 6 esercitazioni di tipo *table-top* a favore di tali organizzazioni, nonché 2 esercitazioni di carattere tecnico a favore del CSIRT Italia, che ha previsto anche l'impiego di un cyber range, ossia di ambienti virtuali nei quali possono essere simulati, a livello tecnico, reti e sistemi informativi oggetto di attacchi.

55 Al riguardo, in modo approfondito, Rossa 2022a: 167 e ss.

ligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia.

Tale previsione – che è stata espunta dal testo nel corso dei lavori parlamentari e, allo stato, è stata riproposta nella più adeguata sede del disegno di legge sull'intelligenza artificiale in discussione al Senato[56] – ha il pregio di assegnare all'ACN la promozione di ogni iniziativa anche di *partenariato pubblico privato*, aprendo la via ad una più ampia collaborazione tra pubblico e privato nel contesto dei contratti pubblici anche al fine di consentire alle amministrazioni di rivolgersi al mercato, come già evidenziato in dottrina[57], per l'approvvigionamento non solo di servizi o prodotti già esistenti sul mercato ma anche per soddisfare l'esigenza di sviluppare *ex novo* prodotti, servizi o lavori innovativi di servizi innovativi, valorizzando istituti come il partenariato per l'innovazione di cui all'art. 75 del d.lgs. n. 36/2023[58].

Nel contesto della cybersicurezza, considerate la debolezza strutturale della PA nell'approvvigionamento dei beni e dei servizi e la trasversalità e l'aumento costante della minaccia e degli incidenti cyber, la riflessione sull'utilizzo dei contratti pubblici come "strumenti creatori di innovazioni" [59], già ampiamente sviluppata in dottrina[60], non sembra ancora essere stata colta pienamente dal legislatore nazionale.

5. Cenni conclusivi

A fronte di una realtà nella quale la minaccia cibernetica cresce, come visto, in termini quantitativi ed è suscettibile di impattare sul complessivo apparato amministrativo, la promozione di forme di collaborazione tra pubbliche amministrazio-

56 Si fa riferimento al disegno di legge A.S. 1146, presentato dal Governo in data 20 maggio 2024 e, al 13 giugno 2024, in corso di esame in commissione. Si veda anche il Dossier n. 289 del Servizio Studi dell'11 giugno 2024, disponibile al link *https://www.senato.it/japp/bgt/showdoc/19/DOSSIER/0/1419908/index.html*.

57 Al riguardo, Rossa 2022a: 205, rileva che uno dei vantaggi derivanti dall'utilizzo degli appalti innovativi – tra i quali il partenariato per l'innovazione ai sensi dell'art. 75 del d.lgs. n. 36/2023, è "la possibilità di soddisfare i fabbisogni pubblici in modo sartoriale, prescindendo da un bene o un servizio già esistente ma potendo invece crearne uno che risponda esattamente alle specifiche esigenze del caso particolare. Infatti, come accennato in precedenza, non sempre la soluzione che offre il mercato è la migliore o quella che serve nel caso specifico: tuttavia, ricorrere a quello che offre il mercato è tendenzialmente la scelta obbligata. Ma non se si ha la possibilità di avvalersi di appalti innovativi come il partenariato per l'innovazione. Il progettare *ab initio* una soluzione o un bene sulle reali esigenze e fabbisogni del soggetto pubblico sarebbe in modo evidente funzionale alle esigenze che possono derivare dal contesto cybersecurity pubblica, sempre in continua evoluzione134. In tal senso, gli appalti innovativi, partenariato per l'innovazione in particolare, potrebbero essere utili per sviluppare prodotti e servizi digitali cybersafe by design, ovvero rispettosi di standard di cybersicurezza già dalla loro progettazione". Condivide tale soluzione anche Longo 2024: 5.

58 Per un approfondimento di tale procedura di scelta del contraente, cfr. Senzani 2024: 413-415.

59 Auby 2022,133.

60 Kondu, James, Rigby 2022: 490-502; Licata 2019: 1 e ss.; Racca 2017:192 e ss.; Racca & Yukins 2019: 113 e ss.; Laimer, Pagliarin & Perathoner 2021: *passim.*

ni e tra privati e amministrazioni e la diffusione di una cultura della cybersicurezza appaiono necessarie per assicurare un più elevato livello di sicurezza. Esse determinano, infatti, un maggiore scambio di conoscenze, di strategie e di soluzioni tecniche, nonché una maggiore sensibilizzazione e responsabilizzazione del capitale umano all'interno delle amministrazioni e della collettività, contribuendo a ridurre la vulnerabilità dell'apparato amministrativo e le conseguenze pregiudizievoli sia per interessi pubblici sia per quelli privati.

Dalla breve analisi condotta su alcune delle più recenti tendenze normative in materia, emerge una progressiva presa di consapevolezza, da valutare con favore, circa la necessità di rafforzare l'organizzazione delle strutture e del sistema amministrativo nei diversi livelli di governo e in molteplici settori e, al contempo, promuovere una procedimentalizzazione delle attività amministrative al fine di prevenire e gestire i rischi e gli incidenti cyber, mediante l'individuazione di ruoli, responsabilità e piani di azione.

Se gli obiettivi sono senz'altro ambiziosi e condivisibili, oltre che imprescindibili per la transizione digitale, non altrettanto condivisibile e piuttosto insoddisfacente è la scelta del legislatore di pretendere di perseguire tali finalità senza nuovi o maggiori oneri a carico della finanza pubblica, come emerge dall'art. 24 della legge n. 90/2024.

Peraltro tale prassi, stigmatizzata anche rispetto ad altri interventi dalla Consulta[61], lascia in ombra quanto già espresso in più occasioni dalla Corte dei conti, ossia che la mera apposizione di clausole di neutralità non costituisce garanzia dell'assenza di nuovi o maggiori oneri e ciò, in quanto, "La mancata previsione, infatti, di costi aggiuntivi non esclude che possano effettivamente derivare dalle norme, in futuro, maggiori esigenze a legislazione vigente, con copertura a carico dei tendenziali e dunque aggravando il saldo, soprattutto a fronte di oneri di carattere obbligatorio. Tutto ciò a meno di non ritenere che le disponibilità di bilancio a legislazione vigente siano quantificate in modo da presentare già margini per la copertura di eventuali incrementi di oneri conseguenti all'implementazione delle nuove normative previste: in tal caso si determinerebbe, però, una scarsa coerenza con il principio della legislazione vigente, che, anche nel nuovo sistema contabile, costituisce il criterio per la costruzione delle previsioni di bilancio al netto della manovra, come attesta la presenza, nella legge di bilancio, della Sezione II, dedicata, appunto, alla legislazione vigente"[62].

61 Al riguardo, di recente, Corte cost., 2 maggio 2023, n. 82, ove la Corte ha ribadito, peraltro, che "la clausola di invarianza finanziaria non può tradursi in una mera clausola di stile e che, «[o]ve la nuova spesa si ritenga sostenibile senza ricorrere alla individuazione di ulteriori risorse, per effetto di una più efficiente e sinergica utilizzazione delle somme allocate nella stessa partita di bilancio per promiscue finalità, la pretesa autosufficienza non può comunque essere affermata apoditticamente, ma va corredata da adeguata dimostrazione economica e contabile» (sentenza n. 115 del 2012), consistente nell'esatta quantificazione delle risorse disponibili e della loro eventuale eccedenza utilizzabile per la nuova o maggiore spesa, i cui oneri devono essere specificamente quantificati per dimostrare l'attendibilità della copertura".

62 Corte dei conti, SS.RR. in sede di controllo, Relazione quadrimestrale sulla tipologia

Al riguardo, ci si limita ad osservare che, considerato l'apparato sanzionatorio previsto dal nuovo testo normativo, non pare potersi escludere che molte delle previsioni introdotte rappresentino oneri di carattere obbligatorio per le amministrazioni coinvolte, richiedendo alle stesse, a titolo esemplificativo, di adeguare le dotazioni *hardware* e *software* in conseguenza di eventuali segnalazioni dell'ACN di rischi di vulnerabilità informatica ovvero di svolgere nuovi compiti, come la raccolta, la elaborazione e la classificazione dei dati relativi alle notifiche di incidenti informatici in capo all'ACN, ovvero di rendere operativo il Centro nazionale di crittografia e di individuare una struttura referente per la cybersicurezza con risorse dotate di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.

In conclusione, appare chiaro che l'ambizioso piano avrebbe richiesto un ingente investimento in termini di risorse finanziarie che, seppur sollecitato da più parti nel corso dei lavori parlamentari, non è stato purtroppo previsto e ciò potrebbe compromettere la sostenibilità amministrativa dell'intervento e la effettiva possibilità di realizzare il fine ultimo dello stesso, ossia il rafforzamento della cybersicurezza nazionale.

Bibliografia

Arcidiacono L. 1974, *Organizzazione pluralistica e strumenti di collegamento. Profili dogmatici*, Milano: Giuffrè.

Auby J.B. 2022, "Conclusioni", in R.C. Perin, M. Lipari & G.M. Racca (a cura di), *Contratti pubblici e innovazioni per l'attuazione della legge delega*, Napoli: Jovene: 133.

Battini, S. 2021, "Premessa", *Formare la PA. Rapporto SNA 2017-2020*, Roma: Miligraf Edizioni: 11-14.

Bazoli, G. 1964, *La collaborazione nell'attività amministrativa*, Padova: Cedam.

Benvenuti F. 1994, *Il nuovo cittadino. Tra libertà garantita e libertà attiva*, Venezia: Marsilio.

Bolognini L., Pelino E. & Scialdone M. 2023 (a cura di), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Milano: Giuffrè.

Bonetti T. 2022, *La partecipazione strumentale*, Bologna: Bologna University Press.

Borriello G. & Fristachi G. 2022, "Stato (d'assedio) digitale e strategia italiana di cybersicurezza", *Rivista di Digital Politics*, vol. II, 1-2: 157-178.

Carotti B. 2020, "Sicurezza cibernetica e Stato-nazione", *Giorn. Dir. amm.*, 629-642.

Chiappini A. 2022, "Quadro normativo in materia di sicurezza informativa e ruolo dell'Agenzia per la cybersicurezza nazionale", in G. Dalia e M. Panebianco (a cura di) 2022, *Il segreto di Stato. Una indagine multidisciplinare sull'equo bilanciamento di ragioni politiche e giuridiche*, Torino: Giappichelli Editore: 301-334.

Chirulli P. 2023 [2015], La partecipazione a procedimento, in M.A. Sandulli (a cura di), *Principi e regole dell'azione amministrativa*, Milano: Giuffrè: 399-411.

Cognetti S. 2000, *"Quantità" e "qualità" della partecipazione, Tutela procedimentale e processuale*, Milano: Giuffrè.

delle coperture e sulle tecniche di quantificazione degli oneri nel quadrimestre, maggio-agosto 2023, Delibera n. 32/2023, pp. 3 e ss.

D'Angelo F. 2022a, *Pluralismo degli enti pubblici e collaborazione procedimentale. Per una rilettura delle relazioni organizzative nell'amministrazione complessa*, Torino: Giappichelli.
D'Angelo F. 2022b, "La collaborazione amministrativa nella funzione di vigilanza (bancaria). Profili di giurisdizione e procedimentali (nota a Cass SU 20 aprile 2021, n. 10355)", *Dir. e proc. amm.*:1.
Fiornelli G. & Giannelli M. 2024, "Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2", *Rivista italiana di informatica e diritto*, 1.
Forgione I. 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", *Dir. Amm.*, 4, 1141.
Giannini M.S. 1983, *Pianificazione* (voce), *Enc. Dir.*, XXXIII: 629.
Giannini M.S. 1973, "Enti locali territoriali e programmazione", *Rivista Trimestrale di Diritto Pubblico*, 1: 193-218.
Giannini M.S. 1961, "Intervento", in *Coordinamento e collaborazione nella vita degli enti locali. Atti del V° Convegno di Studi di Scienza dell'Amministrazione*, Milano: Giuffrè: 114-119.
Giovenco L. 1961, "Profilo giuridico strutturale del «coordinamento» nella vita degli enti locali, in *Coordinamento e collaborazione nella vita degli enti locali. Atti del V° Convegno di Studi di Scienza dell'Amministrazione*, Milano: Giuffrè: 280-286.
Kondu O., James A. & Rigby J. 2020, "Public Procurement and innovation: a systematic literature review", *Science and Public Policy*, 47(4): 490-502.
Laimer S., Pagliarin C., Perathoner C. 2021, *Contratti pubblici e innovazione, Una strategia per far ripartire l'Europa*, Milano: Giuffrè.
Ledda F. 1993, "Problema amministrativo e partecipazione al procedimento", *Dir. Amm.*, 2: 133-172.
Licata G.F. 2019, "Contratti pubblici e innovazione", Convegno Associazione Italiana dei Professori di Diritto Amministrativo. Disponibile in *www.aipda.it*, Paper.pdf (accesso il 18 giugno 2024).
Longo E. 2024, "*Audizione informale per il disegno di legge in materia di "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717), Camera dei Deputati, Commissioni riunite I e II – Roma 28 marzo 2024*", *Riv. Italiana di Informatica e diritto*, 1: 4.
Manganaro F. 1995, *Principio di buona fede e attività delle amministrazioni pubbliche*, Napoli: Edizioni Scientifiche Italiane.
Nigro M. 1966, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano: Giuffrè.
Nigro M. 1980, "Il nodo della partecipazione", *Riv. trim. dir. proc. civ.*: 231 ss.
Police A. 2021, "Enti pubblici di Ricerca ed università: le persistenti ragioni di una differenziazione e le indifferibili esigenze di uno sforzo comune, *Nuove Autonomie*, 1: 65-79.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", *Federalismi.it*, 25: 65-93.
Racca G.M. 2017, "La contrattazione pubblica come strumento di politica industriale", in C. Marzuoli e S. Torricelli (a cura di), *La dimensione sociale della contrattazione pubblica. Disciplina dei contratti ed esternalizzazioni sostenibili*, Napoli: Editoriale Scientifica: 192 e ss.
Racca G.M. & Yukins C. (editors) 2019, "Joint Public Procurement and Innovation: Lessons Across Borders", *Droit Administratif/Administrative Law Collection*, 27, Bruxelles: Bruylant.
Ramajoli, M. 2021, "La Scuola Nazionale dell'Amministrazione agente interno dell'innovazione amministrativa", *Giornale di diritto amministrativo*, 4, 451-456.

Ricotta F.N. 2023a, "L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale, in G. Colaiacovo (a cura di) 2023, *Sicurezza, informazioni e giustizia penale*, Pisa: Pacini Giuridica: 356 ss.

Ricotta F.N. 2023b, "Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria", *Dir. pen. Cont. – Rivista trimestrale*, 1, 97 ss.

Rossa S. 2023a, *Cybersicurezza e pubblica amministrazione*, Napoli: Editoriale Scientifica.

Rossa S. 2023b, "Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario", *Vergentis. Revista de Investigación de la Cátedra Internacional Conjunta Inocencio III*, 17: 161-175.

Rossa S. 2021, *Contributo allo studio delle funzioni amministrative digitali. Il processo di digitalizzazione della Pubblica Amministrazione e il ruolo dei dati aperti*, Milano: Wolters Kluwer-CEDAM.

Scoca F.G. 1990, *Contributo sulla figura dell'interesse legittimo*, Milano: Giuffrè.

Senzani D. 2024, "Il procedimento ad evidenza pubblica e le procedure di scelta del contraente", in F. Mastragostino e G. Piperata (a cura di), *Diritto dei contratti pubblici. Assetto e dinamiche evolutive alla luce del decreto legislativo n. 36/2023*, IV ed., Torino: Giappichelli: 413-415.

Spasiano M.R. 2021, "Nuovi approdi della partecipazione procedimentale nel prisma del novellato preavviso di rigetto", *Il diritto dell'economia*, 67, 105, 2: 25-54.

Tarullo S. 2008, *Il principio di collaborazione procedimentale. Solidarietà e correttezza nella dinamica del potere amministrativo*, Torino: Giappichelli.

Terracciano S. 2023, *Le sanzioni amministrative a tutela degli interessi pubblici procedimentali*, Napoli: Editoriale scientifica.

Torchia L. 2023, *Lo Stato digitale*, Bologna: Il Mulino.

Travi A. 1996, "Le forme di cooperazione interlocale, *Dir. Amm.*, 4: 673 ss.

Zito A. 1996, *Le pretese partecipative del privato nel procedimento amministrativo*, Milano: Giuffrè.

Paolo Heritier

Il dilemma della Cybersicurezza, tra reale e virtuale: uno sguardo prospettico. Una postfazione[*]

In questa breve conclusione, rinviando a un'ideale sequenza tra la prefazione e l'introduzione del primo e di questo volume, si intende in particolare dar conto della collocazione dei volumi in una rivista a titolo *Teoria e critica della regolazione sociale* che, aperta a contributi di giuristi, economisti, politologi e pur facendo del contesto della società complessa il suo ambito di riferimento, è frequentata in particolare da filosofi del diritto.

L'ipotesi che si propone come prospettiva per l'evoluzione del tema della cybersicurezza intende allora fornire linee di un possibile significato ampio e generale, in cui, da problema specifico e tecnologico, il dibattito tende a sollevare questioni concernenti la stessa configurazione della società contemporanea legate a essa.

La riflessione sulla cybersicurezza, all'interno della riflessione filosofico giuridica, tende spesso a essere letta come ambito proprio dell'informatica giuridica, nel tentativo di indicare come le tecnologie informatiche e il loro sviluppo, da un lato, le rilevanti questioni giuridiche di disciplina del settore, dall'altro, e l'esigenza di tenere insieme i due profili, richiedesse la competenza in entrambe i saperi, da parte dello studioso che se ne occupava.

La visione da cui qui si muove è in parte differente, provando a far interagire esperti di campi disciplinari anche molto lontani tra loro, con tutte le difficoltà che ciò implica, ma anche con l'interesse che tali incroci di sapere implicano. Come ricordato nella prefazione al primo volume, il convegno da cui i volumi traggono origine ha mirato proprio a questo obiettivo e la duplice pubblicazione, sia pure in modo più circoscritto e più limitato a scrittori prevalentemente di ambito giuridico, ne è testimonianza. Tale premessa spiega la metodologia proposta, e giustifica anche la conclusione, volta a indicare alcuni possibili ulteriori direzioni della ricerca da approfondire.

Il tentativo interdisciplinare che i due volumi provano infatti a percorrere – nell'alternanza di piccoli passi avanti conseguiti e di inevitabili stalli che devono essere messi in conto nel procedere, con risultati complessivi che il lettore dovrà giudicare – è una metodologia in cui il confronto fra le discipline diverse coinvolte, tecnologico-informatica, economico-organizzativa, giuridico-positiva, giungono a far intravedere la necessità di un dialogo fecondo intorno al nuovo contesto in cui i saperi chiamati in causa sono, per così dire, immersi.

* Scritto non sottoposto alla procedura di referaggio doppio cieco.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760168

L'impressione che si ricava da uno sguardo olistico ai due volumi è che la questione della cybersicurezza tenda sempre più a legarsi al, e in qualche modo a sciogliersi nel, classico problema sociale politico e giuridico della sicurezza, in un duplice movimento, per così dire a doppia elica, in cui la società entra in un quadro il cui significato dell'aggettivo 'cyber' e il termine cyberspazio la caratterizzano in modo crescente. Secondo la logica del principio di coproduzione tra tecnica, diritto e scienze sociali, e al seguito dell'apporto dei *Science and Technology Studies*[1], potremmo ripensare al termine cybersicurezza notando proprio due fenomeni da raccordare: il progressivo divenire del cyberspazio, inteso in senso comprendente, come l'ambiente posto tra reale e virtuale, che configura l'esperienza umana nella società contemporanea in quanto tale e l'esigenza speculare di ripensamento della nozione moderna di sicurezza come fondamento stesso delle forme di interazione sociale. 'Cyber' e 'sicurezza', in altre parole, nel loro reciproco avvicinarsi, mediato dalla nozione di 'spazio', si trasformano, divengono altro, configurando un nuovo ambito necessario di saperi che si intrecciano comunicando. Se questa esigenza di allargamento della platea di chi assiste al dibattito in tema è stata recentemente evocata, qui si intende estendere ancora di più questa prospettiva di ricerca, in primo luogo ai giuristi di diversi ambiti disciplinari, ma facendone una questione generale e dunque di interesse filosofico e metodologico. Rileva infatti efficacemente Di Resta, in relazione alla definizione in evoluzione del concetto di cybersicurezza, come corra l'obbligo di rilevare che il *Cyberspazio* sia un concetto più ampio di *internet*, condividendo forti elementi comuni con la nuova strategia europea volta a proteggere il diritto della protezione dei dati e i diritti fondamentali, considerati veri e propri pilastri del futuro mercato digitale che si prevede. In questo senso "il tema della *Cybersecurity* sarebbe una disciplina che non può essere più solo legata ad un dibattito "*militarizzato*" o comunque riservato a pochi esperti del settore"[2]. In quanto disciplina strettamente connessa al fattore umano[3] nell'organizzazione (pubblica o privata), Di Resta auspica che la discussione diventi "più trasparente e multilivello, non solo un dibattito riservato a livello di vertice istituzionale, con un maggior coinvolgimento della società civile, e che sia ispirato a un forte approccio multidisciplinare, poiché la *Cybersecurity* deve includere anche altri esperti – non solo esperti di informatica o di sicurezza informatica – come quelli della protezione dei dati, psicologi o esperti di comunicazione"[4].

Seguendo questa linea, ci chiediamo se il ragionamento dei due autori non sia da spingere addirittura oltre, configurando sullo sfondo la possibilità di un vero e proprio ritorno *filosofico giuridico* dei temi della cybersicurezza, evocando le origini stesse del diritto internazionale (e forse della stessa modernità) fondato nella visione di Grozio, ai tempi incipienti del dibattito sulla regolamentazione (o sull'assenza di essa) dell'*outer space*.

1 Sugli SST ci limitiamo a ricordare Jasanoff 2001.
2 Di Resta, Grassucci in Di Resta 2024: 255.
3 Bossomaier, D'Alessandro, Bradbury 2020.
4 Di Resta, Grassucci in Di Resta 2024: 255-256.

Le questioni che si stagliano sullo sfondo non appaiono solo organizzative, politiche e giuridiche, ma propriamente antropologiche, relative a quale concezione di diritto e di uomo siano implicate nel complesso problema della sicurezza sociale, politica e giuridica, pensata però in un contesto in cui reale e virtuale, umano e artificiale tendono a confondersi e interagire[5].

Si tratta di articolare diversamente, pertanto, la relazione tra ciberspazio e sicurezza nella riflessione filosofico giuridica. Proverò a indicare alcune linee in questa direzione.

La visione reticolare del diritto emersa a inizio millennio[6], successivamente estesa a problematizzare i profili di *governance* inevitabilmente indotti dall'emergere da una profonda trasformazione delle fonti in corso[7], ha condotto in primo luogo i filosofi del diritto a interrogarsi sulla natura estetica[8] e virtuale[9] dell'ordinamento giuridico, legata al modello kelseniano e alla critica della qualificazione giuridica (appunto virtuale) del fatto (reale) accaduto.

La stessa evoluzione del concetto di testo e la dimensione iper-testuale scaturita dalla Rete Internet, rilevante per tutti i giuristi in seguito alle trasformazioni delle banche dati e della conoscenza giuridica disponibili, come seguito *digitale* della tecnica storica della glossa e dal conseguente affermarsi del cyberspazio[10] come luogo sociale di interazione (Second Life, Metaverso), appare la premessa della rivoluzione mediatica digitale. I problemi della sicurezza si rilevano in questo contesto in tutta la loro rilevanza sociogiuridica, prima con l'emergere delle pratiche selvagge di profilazione e di violazione della privacy legati allo strapotere delle *corporation* e all'emergere del capitalismo della sorveglianza[11] e poi in seguito all'onda prepotentemente in corso in corso concessa all'intelligenza artificiale.

Il problema, a un tempo economico, politico e giuridico della sicurezza su cui sorge la stessa concezione del diritto positivo moderno, non può non seguire dunque questo itinerario sul piano *cyber*, configurando un quadro in cui i progetti di meccanizzazione dell'umano, innescati dalla continuità posta tra progetto cibernetico, scienze cognitive[12] e *machine learning*, giungono ad assegnare all'AI un valore salvifico sia dal punto organizzativo ed epistemologico, sia, financo, religioso[13].

La domanda filosofico-giuridica radicale che pone Montanari in un contesto pre-cyber, se la società del benessere intenda oggi barattare la libertà con la sicu-

5 Diversamente sul tema Moallem 2019; Paglia 2024.

6 Due testi quasi contemporanei a inizio millennio, al momento della rivoluzione di Internet, indicavano questa prospettiva rispettivamente dal punto di vista della teoria generale del diritto e della filosofia giuridica: Ost, De Kerchove 2002; Heritier, 2003.

7 Nella sterminata bibliografia mi limito a indicare Lenoble, Maesschalck, 2010; Andronico 2012; Ferrarese 2010.

8 Robilant 1999.

9 Gentile 2005.

10 Tagliagambe 1996.

11 Denunciata dopo un decennio di sostanziale far west nel settore, come è ampiamente noto, sul piano giuridico e politico da Zuboff 2019 e sul piano filosofico da Stiegler 2019.

12 J.P. Dupuy 2015.

13 Pentland, 2015.

rezza[14], e variamente le analisi di Bombelli, Pizzolato e Costa[15], nel porre la tripartizione tra sicurezza attraverso la tecnica (tecnologie securitarie), sicurezza della tecnica (sicurezza dei prodotti tecnici), sicurezza dalla tecnica (rispetto all'uso che altri ne fanno, come la sicurezza del web) precisano un nodo complesso, che chiama in causa una precisa antropologia relazionale moderna necessariamente messa in questione. Il ricorrente ritorno della figura del doppio virtuale della persona e dell'ambiente digitale da abitare, da ultimo nel Metaverso, il gemello digitale[16], sollevano, oltre ai nuovi problemi normativi, un problema antico.

L'individuazione nel fondamento hobbesiano sulla paura della radice della concezione dello stato moderno (il Leviatano), legata anche al principio di precauzione[17], rappresenta una specifica concezione antropologica che mi pare oggi in questione[18]. Specie se analizzata dalla prospettiva che indicava già negli anni Sessanta del secolo scorso Böckenförde, concernente il rilievo secondo il quale lo stato liberale, per amore della libertà, distrugge i presupposti antropologici sui quali pur si fonda. La celebre forma del *dilemma* assume su di sé il paradosso per il quale lo stato si fonda su una dimensione morale condivisa dai cittadini – esattamente quel che giustifica à la Kelsen l'obbedienza dei cittadini alla legge. Tuttavia, la necessità di garantire *per via coercitiva e autoritativa* il fondamento di tale obbedienza implica il paradosso del tornare ad avviarsi verso una via che lo conduce all'implosione della democrazia e del proprio carattere liberale[19]. Ora l'assai noto *dilemma di Böckenförde*, la cui attualità non mi pare possa essere negata oggi, può essere accostato a quello che Buchanan configura come il *paradosso della cybersicurezza*. Una breve analisi dell'argomentazione di Buchanan ci è allora utile a indicare la rilevanza antropologica, e conseguentemente politica e giuridica del problema che affiora dall'incrocio tra i due dilemmi, quello della legittimazione dello stato liberale e della democrazia e quello delle politiche di cybersicurezza investigate in questi volumi. Con una aggiunta, però: inducendoci a interrogaci sull'utilità – seguendo e parafrasando il percorso intellettuale di Jean-Pierre Dupuy[20], applicato però al campo specifico di cui stiamo parlando – di una filosofia della cybersicurezza, da connettere idealmente a una filosofia del diritto, a un'antropologia filosofica e a

14 Montanari 2012: 10.

15 Bombelli 2015; Pizzolato, Costa 2017.

16 Tagliagambe 2022.

17 Dupuy 2011, Sunstein 2010.

18 Mi permetto di rinviare al motto '*homo homini homo*', che intende contrapporsi ai due estremi antropologici dello '*homo homini lupus*' hobbesiano e dello '*homo homini deus*' spinoziano e baconiano (oggi posto alla base della mitizzazione della tecnologia come tecnica di controllo sociale, ben rappresentata dalla proposta di 'fisica sociale' del già citato Pentland). P. Heritier, Homo Homini Homo. *Frammenti di un'antropologia*, 2 voll., in corso di pubblicazione.

19 Böckenförde 2006.

20 L'itinerario del professore di Stanford erede della cattedra di Girard mi pare dunque assai rilevante anche per il tema della cybersicurezza. Se l'applicazione della matrice matematica della teoria del punto fisso endogeno ed esogeno alla filosofica politica e sociale è un tratto costante della produzione dell'epistemologo, è proprio l'analisi del rischio e del principio di precauzione suggerita nella proposta di un "catastrofismo illuminato".

una metodologia delle scienze sociali, come inevitabili esiti della generalizzazione delle problematiche poste.

L'itinerario del professore di Stanford, infatti, erede della cattedra di Girard ma anche allievo di von Foerster e Illich, se realizza già al suo interno una forte interdisciplinarità, mi pare dunque assai rilevante anche per il ripensamento del tema della cybersicurezza. Pur se non appare certo possibile svolgere l'analisi del *catastrofismo illuminato* in questa sede, occorre limitarsi a qualche breve cenno. Se infatti l'applicazione della matrice matematica della teoria del punto fisso endogeno ed esogeno alla filosofica politica e sociale è un tratto costante della produzione dell'epistemologo[21], è proprio l'analisi del rischio e del principio di precauzione suggerita nella proposta di un "catastrofismo illuminato"[22], volto a pensare in un dossier per il governo francese l'utilizzo possibile del principio di precauzione all'inizio del terzo millennio, a costruire la base predittiva per l'analisi della piccola metafisica degli tsunami[23], culminata poi nel saggio di metafisica dedicato recentemente alla guerra nucleare[24].

L'elemento che mi pare interessante da ricercare nella teoria del catastrofismo illuminato dupuiano è proprio la logica di azione predittiva, a un tempo sistemica e antropologica, che egli propone, a fronte dell'uso delle tecnologie e del problema del male nelle relazioni umane[25]. La proposta metodologica si pone infatti precisamente a quel livello fondativo che il dilemma di Böckenförde solleva come problema per le democrazie contemporanee, nell'occuparsi precisamente degli effetti antropologici diffusi della logica della paura e della necessità di un patto sociale, da non condurre più esclusivamente secondo le analisi hobbesiane dello *homo homini lupus*. La presa in conto contemporanea del *dilemma di Böckenförde* e del *paradosso della cybersicurezza* di Buchanan che stiamo per analizzare, mi sembra quindi poter contenere il rinvio a una concezione diversa del diritto e della metodologia dell'interazione sociale regolata. Tale analisi filosofico giuridica, tuttavia, mi pare promettente proprio anche in relazione alla comprensione effettiva delle problematiche complessive che la gestione degli aspetti a un tempo privatistici e pubblicistici, nazionali e internazionali, tecnologici e antropologico-gestionali, che la questione della cybersicurezza fa emergere. La prospettiva che mi pare dischiudersi, e che debba essere portata avanti ben oltre questi due volumi in ottica interdisciplinare, indica che la cybersicurezza non possa affatto essere ridotta a un mero aspetto tecnologico, gestionale, normativo, ma alluda alla necessità di concepire un nuovo paradigma di riflessione politico e fondativo delle democrazie. Tema, questo, che già il conflitto tra prevenzione e precauzione, e l'emergere dell'intelli-

21 Dupuy 2009. Per un'esposizione sintetica del tema e della sua rilevanza giuridica mi permetto di rinviare a Heritier 2012: 125-136.

22 Dupuy 2011. Testo da me tradotto.

23 Dupuy 2006.

24 Dupuy 2022.

25 Dupuy 2015, e 2010, testi tradotti da me, ove l'autore ricostruisce l'ideologia tecnologica cibernetica posta alla base delle scienze cognitive (e, mi permetto di aggiungere, della contemporanea intelligenza artificiale) e della problematica politica del male e della paura.

genza artificiale come tecnologia dall'impatto sociale rilevante, chiede di prendere in conto in termini generali e propriamente filosofici[26].

Limitiamoci dunque a indicare conclusivamente come il problema del dilemma di Böckenförde possa essere duplicato nel paradosso della cybersicurezza, indicato in un recente testo[27].

Muovendo dal presupposto che il tema del cyber hacking rilevi oggi anche della disciplina delle relazioni internazionali, Buchanan precisa il dilemma riferendosi al celebre episodio della Baia dei Porci nel 1962, in cui il mondo si è avvicinato realmente a un conflitto nucleare tra Stati Uniti e Russia.

Il dilemma politico e relazionale già presente in quel potenziale conflitto è costituito dal fatto che quella che i primi ritenevano costituire un'attività difensiva benigna fosse stato interpretato dai sovietici impauriti come una traiettoria di volo, effettuata dal pilota americano apparentemente aggressiva, e dunque da considerare una seria minaccia[28]. L'autore legge la situazione come *paradigmatica della crisi* proprio di un sistema di sicurezza nucleare, oggi ritornato drammaticamente attuale dopo l'invasione dell'Ucraina da parte della Russia e l'evocazione conseguente dello spettro della guerra nucleare, legato appunto al fraintendimento delle reali intenzioni dell'avversario. Buchanan sostiene che la medesima logica può essere vista all'opera nei processi decisionali propri degli Stati relativi alla cybersicurezza, specie in un contesto di riemergere di un mondo a blocchi contrapposti economici e militari, dopo la crisi della globalizzazione[29]. Sinteticamente, i tre pilastri che l'autore propone per l'analisi del paradosso sono rappresentati:

– dal fatto che il desiderio degli Stati per operazioni future di cybersicurezza spinge ad agire in anticipo per rendere tali operazioni possibili[30] e, conseguentemente, di fronte all'azione similare di altri stati, ci si trova di fronte a un dilemma di interpretazione delle intenzioni simile a quello della baia dei Porci (preparazione di un attacco o semplice misura "preventiva" priva di attuali intenzioni malevoli?);

– dal fatto che gli stati hanno ragioni che sono realmente difensive per lanciare intrusioni informatiche nelle reti di altri stati, al fine di migliorare i propri sistemi raccogliendo informazioni utili e scoprendo futuri rischi tramite attività che possono rimanere del tutto nascoste[31];

– infine dalla tendenza, in tale situazione di ambiguità delle intenzioni, a sbagliare sul lato della cautela, pensando al peggio[32].

Sulla base di tali pilastri analitici, la conclusione di Buchanan è che il paradosso della cybersicurezza, legato all'ambiguità di interpretazione del comportamento

26 Galletti, Zipoli Caiani 2024.
27 Buchanan 2016.
28 Buchanan 2016: 15-16.
29 "Ognuno degli elementi che hanno governato il caso della Guerra Fredda ed altri ancora, come la natura anarchica del sistema internazionale, la necessità per gli Stati di predisporre le proprie abilità e i sistemi di *intelligence*, e il rischio sempre presente di un'interpretazione errata e di un'escalation, ha un'enorme rilevanza nella cybersecurity". Buchanan 2016: 17.
30 Buchanan 2016: 48.
31 Buchanan 2016: 72.
32 Buchanan 2016: 96.

dell'avversario, tenderà a aumentare di rilevanza, nella dinamica delle relazioni internazionali[33]: non solo in caso di crisi, ma anche nella mera previsione di una crisi possibile, implicando investimenti in strategie aggressive, formazione del personale, unità militari di cibersicurezza, e finendo per generare nuova paura[34]. Il paradosso può insomma condurre a risultati che nessuno stato realmente desidera, senza che si intraveda la possibilità di individuare una via di uscita facile[35].

Se l'analisi di Buchanan è verosimile, non è difficile notare come la forma del paradosso raggiunga il dilemma di Böckenförde, indicando una situazione potenzialmente erosiva nella stessa relazione umana: ove il progresso rischia di generare dinamiche in grado di distruggere la società. Ove la distruzione è letterale nel caso di una guerra nucleare, semplicemente metaforica nel caso della crisi dello stato liberale e della democrazia e nella difesa dai cyberattacchi (anche se la vicinanza tra questi ultimi e la guerra nucleare apre scenari certo imprevisti). Entrambe le soluzioni rinviano a una riproposizione del patto sociale, e dunque all'ipotesi che evoluzione della cybersicurezza e crisi dello stato liberale rappresentino due differenti versioni dello stesso problema: la difficile articolazione di libertà e sicurezza. Problemi che domandano di pensare, a parere di chi scrive, a nuove forme di risposte non più riferite allo scenario moderno delineato da Hobbes e relativo alla fondazione della norma sulla paura e sulla sanzione (scenario che sembra l'esito del ritorno al principio di precauzione di fronte alle catastrofi, da quella climatica a quella nucleare).

Così, appare possibile estendere, conclusivamente, la logica del paradosso della cybersicurezza in altre direzioni. Le particolarità della dinamica delle relazioni internazionali indica una logica di fondo che, tenendo conto ovviamente delle differenze di situazioni, di investimenti, di attori protagonisti, di circostanze, può differentemente configurarsi anche nelle relazioni private e pubbliche, proprio a partire dalla sostanziale pervasività che si annuncia dei problemi di cybersicurezza, in una società che si approssima a sciogliere, forse definitivamente, la distinzione tra reale e virtuale in una realtà aumentata, sia essa propria del Metaverso[36] o di altre fattezze oggi ancora ignote, in cui il limite tra presenza fisica e presenza virtuale diventerà sempre più elastico e sfumato.

Se già infatti sono stati resi noti casi di "reati" relativi a offese verso la "persona" (ad es. stupri virtuali) commessi nel Metaverso, il problema stesso della cybersicurezza tende a divenire, per la sua articolata dimensione che si estende dal profilo delle relazioni tra stati a quelle fra privati, una questione di sicurezza trasversale, che dai sistemi di sicurezza informatica si volge fino alla stessa "corporeità virtuale" (qualsiasi cosa possa significare l'ossimoro). In una possibile riproposizione del problema di fondo dell'antropologia moderna da cui scaturiscono i diritti dell'uomo, e che, come ha precisato Böckenförde, è alla base del dilemma dello Stato liberale, nel suo connettere libertà e sicurezza.

33 Buchanan 2016: 155.
34 Buchanan 2016: 188.
35 Buchanan 2016: 194.
36 Tagliagambe 2022.

Se la proposta di una filosofia della cybersicurezza, che mi pare al tempo stesso una filosofia del diritto, mi pare implicita nella proposta di Dupuy di un *catastrofismo illuminato*, molte altre riflessioni si prospettano come necessarie di fronte a un cambio di paradigma radicale nella concezione stessa nel giuridico e nelle relazioni sociali, politiche ed economiche tra uomini, che, intravisto all'orizzonte, si sta avvicinando in modo sempre più veloce. È a tale orizzonte che, mi pare, che la riflessione tecnologica, organizzativa e istituzionale sulla cybersicurezza si debba altrettanto rapidamente confrontare, fornendo nuove soluzioni sociali (e non solo tecnologiche, o normative) innovative a vecchi problemi fondamentali, e non limitandosi a seguire la riproposizione di logiche di potere che appaiono oramai consunte, in primo luogo dal punto di vista delle relazioni umane che presuppongono: configurando un nuovo settore di studi autenticamente interdisciplinari e critici.

Bibliografia

Andronico A. 2012, *Viaggio al termine del diritto*. *Saggio sulla* governance, Torino: Giappichelli.

Böckenförde E.W. 2006, *Stato, costituzione, democrazia. Studi di teoria della costituzione e di diritto costituzionale,* Milano: Giuffrè.

Bossomaier T. D'Alessandro S. Bradbury R. 2020, *Human Dimension of Cybersecurity,* Baca Raton, London, New York: CRC Taylor and Francis.

Bombelli G. 2015, *Circuiti pericolosi. La sicurezza tra potere, mercato, e contesti postmoderni. Annotazioni filosofico-giuridiche* in Pizzolato F. Costa P. (a cura di), *Sicurezza, stato e mercato,* Milano: Giuffrè.

Buchanan B. 2016, *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations,* New York: Oxford University Press.

Dupuy J.-P. 2006, *Piccola metafisica degli tsunami. Male e responsabilità nelle catastrifi del nostro tempo*, Roma: Donzelli.

Dupuy J.-P. 2009, *Dans l'oeil du cyclone. Colloque de Cerisy,* ed. Anspach M., Paris: Carnets Nord.

Dupuy J.-P. 2010, *Avevamo dimenticato il male? Pensare la politica dopo l'11 settembre,* Torino: Giappichelli.

Dupuy J.-P. 2011, *Il catastrofismo illuminato. Quando l'impossibile è certo,* Milano: Medusa.

Dupuy J.-P. 2015, *All'origine delle scienze cognitive. La meccanizzazione della mente,* Milano: Mimesis.

Dupuy J.-P. 2022, *La guerre qui ne peut pas avoir lieu, Essai de métaphysique nucléaire,* Paris: Desclée de Brouwer.

Ferrarese M. R. 2010, *La* Governance *tra politica e diritto*, Bologna: Il Mulino.

Galletti M. Zipoli Caiani S. eds. 2024, *Filosofia dell'Intelligenza Artificiale. Sfide etiche e teoriche,* Bologna: Il Mulino.

Gentile F. 2005, *Ordinamento giuridico, tra reale e virtuale,* Padova: Cedam.

Heritier P. 2003, *La rete figurale del diritto. Materiali per un ipertesto didattico, Urbe Internet, vol. 1*, Torino: Giappichelli (Theleme 2001).

Heritier P. 2012, *Estetica giuridica. Vol. 2. A partire da Legendre. Il fondamento finzionale del diritto positivo,* Torino: Giappichelli.

Jasanoff S. 2001, *La scienza davanti ai giudici. La regolazione giuridica della scienza in America,* Milano: Giuffrè.
Kosseff J. 2020, *Cybersecurity Law,* Hoboken: Wiley.
Lenoble J. Maesschalck M. 2010, *Democracy, Law, Governance,* London: Routledge.
Moallem A. ed. 2019, *Human-computer Interaction and Cybersecurity Handbook,* Boca Raton: Crc Taylor and Francis.
Montanari B. 2012, *Capire l'oggi*, in Montanari B., ed. *Luoghi della filosofia del diritto. Idee strutture mutamenti,* Torino: Giappichelli.
O' Connell M. 2018, *Essere una macchina. Un viaggio attraverso cyborg, utopisti, hacker e futurologi per risolvere il modesto problema della morte,* Milano: Adelphi.
Ost F. De Kerchove M, 2002, *De la pyramide au résau? Pour une théorie dialectique du droit*, Bruxelles: Presses Universitaires de Bruxelles.
Paglia V. 2024, *L'algoritmo della vita. Etica e intelligenza artificiale,* Casale Monferrato: Piemme.
Pentland V. 2015, *Fisica sociale. Come si propagano le buone idee,* Milano: Università Bocconi Editore.
Pizzolato F. Costa P. 2017, *Sicurezza e tecnologia,* Milano: Giuffrè.
Resta F. di 2024, *Privacy, data protection, cybersecurity e artificial intelligence,* Roma: Duepuntozero.
Robilant E. di 1999, *Diritto, società e persona. Appunti per il corso di filosofia del diritto 1998-1999,* Torino: Giappichelli.
Stiegler B. 2019, *La società automatica. Vol 1. L'avvenire del lavoro,* Milano: Meltemi.
Sunstein, C.R. 2010, *Il diritto della paura. Oltre il principio di precauzione,* Bologna: Il Mulino.
Tagliagambe S. 1996, *Epistemologia del cyberspazio*, Cagliari: Demos.
Tagliagambe S. 2022, *Metaverso e gemelli digitali. La nuova alleanza tra reti naturali e artificiali* Mondadori: Milano.
Tikk E. Kertunen M. 2020, *Routledge Handbook of International Cybersecurity,* Abingdon, New York: Routledge.
Zuboff S. 2019, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma: LUISS.

Informazioni sugli autori

Giovanni Bombelli, Professore Ordinario di Filosofia del Diritto nell'Università Cattolica del Sacro Cuore

Elena Buoso, Professoressa Associata di Diritto Amministrativo nell'Università degli Studi di Padova

Federica Ceci, Professoressa Ordinaria di Organizzazione Aziendale nell'Università degli Studi G. D'Annunzio

Giovanna Dondossola, Research Project Manager presso Ricerca sul Sistema Energetico – RSE S.p.A.

Paolo Heritier, Professore Ordinario di Filosofia del Diritto nell'Università degli Studi del Piemonte Orientale

Niloofar Kazemargi, Ricercatrice a tempo determinato (RTDA) di Organizzazione Aziendale nell'Università degli Studi G. D'Annunzio

Manfredi Matassa, Assegnista di Ricerca di Diritto Amministrativo nell'Università degli Studi di Palermo

Andrea Mattarella, Dottore di Ricerca in Diritto Penale nell'Università LUMSA di Palermo

Luigi Previti, Ricercatore a tempo determinato (RTDB) di Diritto amministrativo nell'Università degli Studi di Palermo

Lorenzo Ricci, Dottorando in Diritto Amministrativo nell'Università degli Studi della Tuscia

Carla Maria Saracino, Assegnista di Ricerca di Diritto Amministrativo nell'Università degli Studi del Salento

Giuseppe Sferrazzo, Dottorando in Teoria dei contratti, dei servizi e dei mercati nell'Università degli Studi di Roma "Tor Vergata"

Simona Terracciano, Ricercatrice a tempo determinato (RTDB) di Diritto Amministrativo nell'Università degli Studi della Campania Luigi Vanvitelli

Riccardo Ursi, Professore Ordinario di Diritto Amministrativo nell'Università degli Studi di Palermo