Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di

Raffaella Brighi e Giovanna Adinolfi

Giappichelli

Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche


IUSTITIAM COLIMUS

Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di
Raffaella Brighi e Giovanna Adinolfi

Giappichelli

VIA PO, 21 - TEL. 011-81.53.111

http://www.giappichelli.it

ISBN/EAN 979-12-211-1735-6
ISBN/EAN 979-12-211-6531-9 (ebook)

Il volume è esito del progetto di ricerca "Ecocyber - Risk management for future cyber-physical ecosystems" nell'ambito dello Spoke 8 del Paternariato esteso SERICS- SEcurity and RIghts in the CyberSpace.
Finanziato dall'Unione Europea – NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3 – Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca – D. D. 341 del 15/03/2022, PE7 SERICS – SEcurity and RIghts in the CyberSpace , Codice proposta: PE00000014, CUP: J33C22002810001,finanziato con Decreto n. 1556 del 11/10/2022.
I punti di vista e le opinioni espresse sono esclusivamente quelle degli autori e non riflettono necessariamente quelle dell'Unione Europea, né può l'Unione Europea essere ritenuta responsabile per esse.

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

G. Giappichelli Editore

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: LegoDigit s.r.l. - Lavis (TN)

Indice

pag.

Capitolo 3

Il quadro della governance della cybersicurezza a livello nazionale

Tommaso F. Giupponi

pag.

Capitolo 4

La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello *jus ad bellum*

Giulia Gabrielli

Capitolo 5

Il dominio cyber negli attuali scenari di guerra mediterranei: il caso del conflitto in Medio Oriente

Riccardo Allegri, Giorgio Scichilone

Capitolo 6

Politiche di cybersicurezza e implicazioni strategiche: una lettura politologica

Luigi Martino, Giampiero Giacomello, Oltion Preka

pag.

Parte II

Cybersicurezza e protezione degli eco-sistemi cyberfisici: una visione strumentale

Capitolo 7

Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il *Cyber Resilience Act*

Pier Giorgio Chiara

Capitolo 8

Il *Cyber Resilience Act* nella prospettiva degli accordi commerciali dell'Unione europea

Giovanna Adinolfi, Rachele Magnaghi

pag.

Capitolo 9

Profili informatico-giuridici della cybersicurezza nel procurement sanitario

Marco Mancarella

Capitolo 10

Cybersicurezza e *cyber deception*: sfide e prospettive processualpenalistiche

Mariagisa Landolfi

pag.

Parte III

Cybersicurezza e tutela dei diritti fondamentali: una prospettiva critica

Capitolo 11

Polizia, *big data* e società digitale: sicurezza dei dati, sicurezza dai dati

Giulia Fabini

Capitolo 12

Il *Cyber Resilience Act* come strumento per la protezione dei valori dell'UE? Tra esigenze di sicurezza dei prodotti e tutela dei diritti fondamentali dei singoli

Virginia Remondino

pag.

Capitolo 13

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa

Antonio Pugliese, Giulia Lasagni

Parte IV

Consapevolezza, educazione e politiche

Capitolo 14

Cybersicurezza e fattore umano: un approccio educativo inclusivo

Antonella Carbonaro, Enrico Gnagnarella

pag.

Capitolo 15

Per un uso consapevole e sicuro delle tecnologie: strategie educative e strumenti di intervento

Valeria Barone, Thomas Casadei

pag.

Introduzione

Raffaella Brighi, Giovanna Adinolfi

La cybersicurezza gioca un ruolo fondamentale nelle vite dei cittadini. Il funzionamento ordinario della società e dell'ordine democratico, unitamente alle attività economiche e sociali, fa sempre più affidamento sulle reti, sistemi informativi e servizi informatici, nonché dispositivi cyberfisici connessi.

Più la nostra realtà è permeata dalle tecnologie digitali e da approcci basati sul trattamento – anche automatizzato – dei dati, personali e non personali, più le minacce cibernetiche emergono con frequenza e sofisticatezza maggiore, ponendo rischi significativi non solo agli asset materiali di operatori pubblici e privati, ma anche ai diritti e libertà fondamentali dei cittadini, nonché alla sicurezza nazionale. In questo contesto, l'evoluzione dello scenario geopolitico internazionale contribuisce a determinare la rimodulazione delle possibili minacce, anche introducendone di nuove, ad esempio con riguardo alla sicurezza delle catene di approvvigionamento da cui dipendono le infrastrutture critiche.

Al fine di aumentare il livello di resilienza contro queste minacce, nel dicembre 2020 la Commissione europea e l'Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza hanno presentato la terza Strategia dell'UE per la cybersicurezza [1]. La cybersicurezza è ormai una componente chiave ed integrata nelle politiche digitali dell'UE, come reso evidente dal Piano di Transizione Digitale Europeo [2], il Piano per la Ripresa dell'Europa [3] e la

[1] Commissione Europea e Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza, *The EU's Cybersecurity Strategy for the Digital Decade*, (JOIN2020) 18 final.

[2] Commissione Europea, *Shaping EU's Digital Future*, 2020, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en#documents.

[3] Commissione Europea, *Recovery Plan for Europe*, 2020, https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_en.

Strategia Europea di Sicurezza [4] elaborati nel 2020. La strategia del 2020 si fonda sui precedenti documenti programmatici del 2013 [5] – quando la cybersicurezza diviene ufficialmente un'area di politiche unionali [6] – e del 2017.

Dal 2013, la politica dell'Unione europea in materia di cybersicurezza si è sviluppata in modo significativo anche e soprattutto sul versante legislativo. Infatti, con diversi atti giuridici di diritto derivato si è inteso perseguire gli obiettivi di alto-livello identificati nelle Strategie, iniziando dalla direttiva UE 2016/1148 (direttiva NIS) e il regolamento UE 2019/881 (*Cybersecurity Act*), fino alla recente 'ondata' di regolamentazione composta dalla direttiva UE 2022/2555 (direttiva NIS2), direttiva UE 2022/2557 (direttiva CER), regolamento UE 2024/2554 (DORA), regolamento UE 2024/2847 (*Cyber Resilience Act*), regolamento UE 2025/38 (*Cyber Solidarity A*ct). Queste direttive e regolamenti, ancorché abbiano obiettivi ed oggetti diversi, condividono un approccio regolatorio, quello cioè basato sul rischio, che è progressivamente diventato il modello di governance adottato dall'UE nella regolazione in materia digitale [7] già dalla pubblicazione nel 2015 della Strategia sul Mercato Unico Digitale [8].

In questo contesto, il volume approfondisce una serie di importanti sfide normative – giuridiche, etiche e sociali – che emergono nell'ambito della governance della cybersicurezza nell'Unione europea. La prima parte fa luce sui processi dai quali è emerso un diritto della cybersicurezza e sulle sue possibili implicazioni. Dopo aver introdotto il concetto di cybersicurezza, inteso come snodo interdisciplinare in cui convergono saperi giuridici, informatici, ingegneristici e socio-economici, ne viene proposta una valutazione giuridica nella prospettiva del diritto interno italiano e dell'Unione europea, anche in termini comparati rispetto alle esperienze di altri Stati. La dimensione transfrontaliera degli attacchi informatici è indagata con particolare riferimento ai contesti bellici nel quadro delle gravi tensioni dell'area mediorientale e secondo la prospettiva del divieto di uso della forza previsto dal diritto internazionale.

---

[4] COMMISSIONE EUROPEA, *European Security Union Strategy*, (COM2020) 605 final.

[5] COMMISSIONE EUROPEA AND HIGH REPRESENTATIVE, *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace*, (JOIN 2013) 1 final.

[6] G. GONZALEZ FUSTER-L. JASMONTAITE, *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in M. CHRISTEN-B. GORDIJN-M. LOI (eds), *The Ethics of Cybersecurity*, Springer Nature, 2020(97).

[7] G. DE GREGORIO-P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 59(2), 476, 2022; P.G. CHIARA-F. GALLI, *Normative Considerations on Impact Assessments in EU Digital Policy*, in *Medialaws*, 2024(1), 86.

[8] COMMISSIONE EUROPea, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe*, COM(2015)192 final.

L'obiettivo è introdurre il lettore alla complessità di una materia per la quale la regolamentazione elaborata a vari livelli (interno, europeo, internazionale) deve cercare il giusto equilibrio tra profili istituzionali, economico-sociali e tecnico-scientifici.

La seconda parte del volume si propone di esplorare le istituzioni e le norme che regolano la cybersicurezza dei sistemi cyberfisici e dei prodotti con elementi digitali. Tali dispositivi determinano infatti un cambiamento radicale nel panorama della minaccia [9], poiché si collocano all'intersezione tra il mondo fisico e quello digitale. Di fronte alla connettività pervasiva e all'inarrestabile digitalizzazione delle nostre società, questi prodotti rappresentano un'appetibile superficie di attacco, come evidenziato dall'ENISA, che prevede un aumento significativo degli attacchi entro il 2030 [10]. Questi attacchi possono sfruttare dispositivi obsoleti o configurati con impostazioni predefinite per ottenere un accesso iniziale, spostarsi lateralmente attraverso le reti e compromettere reti e dati sensibili. Gli sviluppi legislativi dell'UE vengono esaminati anche alla luce degli obblighi internazionali assunti dall'Unione nei confronti di paesi partner, in particolare nel quadro degli accordi commerciali. Infine, vengono esaminati aspetti di legittimità rilevanti nelle attività di c.d. *cyber deception* nell'ambito dei sistemi cyberfisici.

Nella terza parte la cybersicurezza è indagata nella prospettiva della tutela dei diritti fondamentali. Nel contesto attuale, i fattori di rischio e le minacce si estendono oltre le reti, i sistemi informativi e i dispositivi connessi. La garanzia della sicurezza di questi ultimi si impone anche per tutelare i diritti e le libertà fondamentali degli individui, quali, ad esempio, il diritto alla riservatezza e la protezione dei dati personali, nonché la libertà di espressione. Se, da una parte, è noto che gli attacchi informatici possano violare taluni diritti fondamentali, compromettere l'incolumità fisica e avere conseguenze critiche per il processo democratico di una società, dall'altra, è meno evidente come le misure di cybersicurezza possano avere un impatto negativo sui diritti fondamentali [11]. In relazione a ciò, è necessario anche analizzare in che misura gli atti giuridici dell'UE in materia di cybersicurezza tutelino effettivamente i diritti fondamentali. Infine, viene investigato l'utilizzo di dati e informazioni di cybersicurezza nel contesto del procedimento penale, in particolare se raccolti nel quadro di attività amministrative.

---

[9] Si veda P.G. CHIARA, *The Internet of Things and EU Law: Cybersecurity, Privacy and Data Protection challenges*, Springer, 2024.

[10] ENISA, *Identifying Emerging Cyber Security Threats and Challenges for 2030*, 2023, 14.

[11] M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds and Machines*, vol. 29, 2019, 3, 352; M. HILDEBRANDT, *Digital security and human rights: a plea for counter-infringement*, in M. SUSI (ed.), *Human Rights, Digital Society and the Law: A Research Companion*, Taylor & Francis, 2019, 266.

La quarta e ultima parte del volume si concentra sul fattore umano. Se l'errore umano rimane la principale causa degli incidenti, diventa essenziale aumentare la consapevolezza sulle questioni digitali e di cybersicurezza. Non solo i dipendenti pubblici e i lavoratori del settore privato, ma anche gli individui nel loro complesso, come parte della società, devono essere in grado di riconoscere le potenziali minacce e adottare pratiche online più sicure, poiché il rischio cibernetico può avere effetti di ricaduta drammatici. A questo proposito, è fondamentale riconoscere le potenziali barriere agli sforzi educativi, come l'accesso limitato, i costi, i pregiudizi intrinseci e le norme socioculturali, che contribuiscono al divario digitale o alle disparità di genere.

Questo volume figura tra i risultati del progetto di ricerca **EcoCyber – *Risk Management for Future Cyber-Physical Ecosystems***, coordinato dal Prof. Michele Colajanni (Università di Bologna, Dipartimento di Ingegneria e Scienza dell'informazione) nell'ambito del Partenariato esteso SERICS – *Security and Rights in the CyberSpace* (finanziato dall'Unione Europea, NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR, Missione 4 Componente 2, Investimento 1.3). SERICS ha la missione di sviluppare ricerca di base su *Cybersecurity, nuove tecnologie e tutela dei diritti*.

In questa cornice, le ricerche condotte per il progetto EcoCyber dal 2023 hanno affrontato le sfide di sicurezza e resilienza dei futuri ecosistemi cyberfisici con un approccio realmente multidisciplinare, che ha intrecciato prospettive tecniche, giuridiche, etiche, politiche e sociologiche.

La ricerca si è sviluppata lungo quattro direttrici complementari: i primi tre filoni hanno prodotto studi, modelli e metodi volti a migliorare la gestione continua del rischio, a delineare soluzioni tecniche per componenti digitali più sicure e architetture orientate alla resilienza.

Al centro del presente volume vi sono, invece, alcuni degli approdi della quarta direttrice "***Rules for the Future Society* (WP4)**", coordinata dal Dipartimento di Scienze Giuridiche dell'Università di Bologna in sinergia con il Dipartimento di Scienze Politiche e Sociali e il Dipartimento di Ingegneria e Scienza dell'informazione dell'Università di Bologna e con il Dipartimento di Studi Internazionali, Giuridici e Storico – Politici dell'Università di Milano.

La ricerca in questo ambito ha affrontato la dimensione giuridica, politica e sociale della governance del rischio *cyber*, con un'analisi critica dei quadri normativi europei e nazionali, delle certificazioni e degli standard tecnici, mettendo in luce le tensioni tra esigenze di sicurezza e tutela delle libertà individuali. In sinergia con i gruppi tecnici è stata inoltre elaborata una guida interattiva, basata su metodologie di *legal design*, dedicata al *Cyber Resilience Act* dell'Unione europea, pensata per offrire uno strumento di consultazione chiaro e accessibile. Un ulteriore risultato, rilevante sul piano sociale, riguarda la promozione del-

l'educazione digitale e della formazione, con iniziative mirate a colmare il divario di genere attraverso percorsi educativi e professionali dedicati.

Hanno apportato un contributo significativo alle attività anche tre progetti risultati vincitori dei bandi a cascata di EcoCyber, sulla linea di ricerca "*Rule, norms, and policies for the protection of the future society*". I contributi raccolti in questo volume ne riflettono i risultati: il progetto SAFELY – *Social media Awareness For Education and Legal Youth* dell'Università di Modena e Reggio Emilia (Prof Thomas Casadei, CRID – Centro di Ricerca su Discriminazione e vulnerabilità); il progetto AcySeM – *Assessing Cyber Security Maturity in National and Legal Frameworks: A Multidisciplinary Approach to Protecting National Critical Infrastructures in Italy and Europe*, dell'Università di Palermo (Prof. Giorgio Scichilone, Dipartimento di Scienze Politiche e delle Relazioni Internazionali); e infine *ILACY – Italian Law for a Cyber-physical ecosystem*, presso l'Università del Salento (Prof. Marco Mancarella, Dipartimento SUS). Queste ricerche hanno arricchito il lavoro del WP4, offrendo prospettive giuridiche e multidisciplinari che si inseriscono pienamente nel percorso del progetto EcoCyber.

In questa prospettiva, il progetto **EcoCyber** non si è limitato a proporre soluzioni tecnologiche, ma ha restituito una visione olistica della sicurezza digitale, nella quale la resilienza dei sistemi dipende tanto dall'innovazione tecnica quanto dalla capacità di rinnovare quadri normativi, politiche pubbliche e modelli sociali.

Concludiamo questa introduzione al volume ringraziando sinceramente i colleghi e le colleghe che hanno contribuito alle attività del WP4. Questo volume vuole rendere testimonianza dello scambio intenso di saperi e interessi che ha caratterizzato questa esperienza. Desideriamo esprimere un ringraziamento speciale ai giovani studiosi e alle giovani studiose che hanno contribuito al progetto, dimostrando un impegno costante e notevole. Infine, rivolgiamo un ringraziamento particolare al dott. Pier Giorgio Chiara, la cui dedizione è stata determinante per il successo dell'iniziativa.

Parte I

L'emersione del diritto alla Cybersicurezza

Capitolo 1

Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica

Raffaella Brighi [*]

Abstract: Il contributo sviluppa una riflessione informatico-giuridica sul concetto di cybersicurezza, inteso come snodo interdisciplinare in cui convergono saperi giuridici, informatici, ingegneristici e socio-economici. Muovendo dall'analisi della sua evoluzione semantica – dall'originaria accezione tecnico-operativa alla progressiva integrazione in ambito normativo e regolamentare – si evidenziano le ambiguità definitorie che caratterizzano il termine e i rischi che tali incertezze comportano per la coerenza del quadro giuridico e per il principio di certezza del diritto. Attraverso un esame comparato delle fonti normative e tecniche, l'indagine mira a delineare un significato coerente e funzionale di cybersicurezza, capace di integrare le diverse prospettive disciplinari e di offrire un riferimento teorico solido tanto per la ricerca quanto per le prassi operative, pur nella consapevolezza dei limiti di una completa armonizzazione.

Keywords: Cybersicurezza – Norme tecniche – Sicurezza informatica – Gestione del rischio – Sistemi cyberfisici

---

[*] Professoressa associata di Informatica giuridica presso il Dipartimento di Scienze Giuridiche dell'Università di Bologna; fa parte del CIRSFD-Centro Human Alma AI, raffaella.brighi @unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

Una riflessione di matrice informatico-giuridica sul concetto di "cybersicurezza" rappresenta un presupposto imprescindibile per ogni attività di indagine e ricerca nel settore, poiché tale concetto si colloca in un'area di intersezione tra saperi eterogenei e coinvolge in modo trasversale discipline giuridiche, informatiche, ingegneristiche e socio-economiche. La sua analisi richiede dunque un approccio integrato e interdisciplinare, capace di coglierne la complessità teorica e operativa, nonché le implicazioni normative, tecniche e applicative.

Sebbene l'espressione "cybersicurezza" si sia ormai consolidata nell'uso comune e specialistico, la sua affermazione come termine autonomo è relativamente recente [1]. Essa compare infatti come neologismo nella Enciclopedia Treccani – italianizzazione del termine *Cybersecurity* – solo a partire dal 2008, a testimonianza di una formalizzazione terminologica piuttosto recente rispetto all'evoluzione tecnologica di riferimento [2]. Originariamente declinato in termini quasi esclusivamente tecnici, il termine "cybersicurezza" ha progressivamente ampliato i propri confini semantici, integrandosi nel quadro normativo e regolamentare e permeando ambiti che travalicano l'informatica. Le tendenze di ricerca rilevate attraverso *Google Trends* indicano un incremento significativo delle *query* associate al termine a partire dal biennio 2016-2017, evidenziandone una crescente diffusione, sia nel dibattito pubblico sia nella riflessione accademica e professionale.

In questo quadro, il concetto di cybersicurezza presenta una significativa variabilità semantica, assumendo significati mutevoli e, in taluni casi, sovrapponibili ad altri termini affini quali (cyber)resilienza o sicurezza informatica [3], e dunque è difficilmente mappabile nel rispettivo concetto in chiave tecnico-scientifica.

Soprattutto in un contesto in cui il diritto viene ad intersecarsi con un sapere scientifico quale è l'informatica, è necessario giungere a un significato uniforme e coerente dei concetti, delle procedure, delle metodologie in uso [4].

---

[1] Per la ricostruzione etimologica del termine cybersicurezza si veda S. ROSSA, *Cybersicurezza e Pubblica Amministrazione*, Edizione Scientifica, Napoli, 2023, p. 9 ss.

[2] Il contenuto della definizione risulta tuttavia piuttosto circoscritto: «Sistema di sicurezza che protegge la rete telematica di uno Stato da eventuali attacchi terroristici perpetrati per via informatica». Voce 'Cybersicurezza', in *Enciclopedia Treccani*, 2008, https://www.treccani.it/vocabolario/cybersicurezza_(Neologismi)/.

[3] L.A. BYGRAVE, *Cyber Resilience versus Cybersecurity as Legal Aspiration*, in T. JANČÁRKOVÁ-G. VISKY-I. WINTHER (a cura di), *14th International Conference on Cyber Conflict*, CYCON, 2022, pp. 27-43.

[4] In una prospettiva più ampia, tale finalità rientra tra gli obiettivi fondanti della Informatica giuridica, nel cui alveo a partire dalla seconda metà del Novecento si sono sviluppate quelle

L'ambiguità concettuale sottesa al termine cybersicurezza potrebbe portare con sé il rischio di minare la coerenza interna del quadro giuridico di riferimento, compromettendo altresì il principio di certezza del diritto. L'assenza di chiarezza terminologica, infatti, può generare incertezze applicative e interpretative, con ripercussioni rilevanti sia sul piano operativo sia su quello delle garanzie giuridiche.

In questa prospettiva, uno degli obiettivi primari di questa indagine è chiarire la semantica e le caratteristiche strutturali del concetto di cybersicurezza nei diversi perimetri applicativi e ricostruirne il significato in modo da offrire un quadro definitorio coerente e funzionale alle esigenze del diritto e della tecnica. La coesistenza di profili tecnici e giuridici, insieme alle intersezioni con altre aree del diritto (sicurezza delle informazioni, criminalità informatica, privacy) e con discipline affini quali sociologia e scienza politica, rende complessa la definizione univoca del termine. È pertanto necessario mettere a sistema le varie accezioni e favorire una comprensione condivisa, pur consapevoli che un'armonizzazione totale tra definizione e prassi applicative potrebbe non essere sempre realizzabile.

L'analisi che segue prende, dunque, le mosse dai paradigmi della sicurezza informatica nella loro dimensione tecnico-scientifica, ricostruendone le prime definizioni e l'evoluzione concettuale. In questa fase la standardizzazione emerge come fattore decisivo di chiarezza semantica e di operatività regolativa. Successivamente, a fronte dei dati forniti da associazioni di settore e agenzie istituzionali – che offrono uno sguardo sull'evoluzione dei rischi globali – l'attenzione si sposterà sull'ampliamento significativo del perimetro da proteggere e dunque sulla affermazione del termine "cybersicurezza". L'esame delle molteplici definizioni adottate da istituzioni e organismi di normazione rivela un mosaico frammentato che sollecita la ricerca di una chiave di lettura unitaria; mentre nel quadro giuridico attuale affiorano due prospettive, complementari ma non prive di tensioni. La riflessione conclusiva restituirà un concetto, cybersicurezza, che si conferma avvolgente, dinamico e mutevole. Prende forma così un modello olistico, capace di andare oltre la riduzione a semplice strumento tecnologico o vincolo normativo: un paradigma integrato, dove dimensioni giuridiche, sociali, economiche e tecniche si intrecciano, delineando una prospettiva sostenibile per affrontare le sfide della società digitale.

---

teorie scientifiche che hanno tracciato le interconnessioni concettuali e operative tra tecnica e diritto. Pionieristiche in Italia le opere di V. FROSINI, *Cibernetica, diritto e società*, Edizioni di Comunità, 1968, e di M.G. LOSANO, *Giuscibernetica. Macchine e Modelli cibernetici nel diritto*, Einaudi, 1969. Per un inquadramento attuale della disciplina si veda *ex multis* G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli, 2022.

2. I paradigmi della sicurezza informatica: sicurezza dei sistemi, delle reti e dei dati

In ambito tecnico scientifico il concetto di cybersicurezza affonda le radici nella sicurezza informatica, disciplina che ha cominciato a delinearsi con maggiore chiarezza tra gli anni '80 e gli anni '90, quando la rapida diffusione delle tecnologie ICT in settori produttivi, istituzionali e privati ha reso evidente l'esigenza di adottare misure specifiche per la protezione di sistemi e dati dalle prime minacce digitali perlopiù riconducibili ad attività di tipo amatoriale o sperimentale, ma comunque segnale precoce dell'esigenza di sviluppare approcci sistematici alla difesa degli ambienti informatici. Successivamente, il panorama delle minacce informatiche si è trasformato con lo sviluppo delle reti e dei servizi informatici, alimentato da motivazioni e strumenti di natura diversa. Nel corso degli anni duemila, l'interconnessione tra server e reti ha reso possibili attacchi distribuiti di tipo *Denial of Service*, talvolta impiegati per fini dimostrativi o di sabotaggio geopolitico (come nei noti episodi in Estonia nel 2007 [5]), mentre spyware, trojan e rootkit hanno iniziato a perseguire obiettivi di raccolta dati e accesso occulto a infrastrutture critiche [6].

In questa fase, la sicurezza informatica si è sviluppata sotto il profilo definitorio e metodologico attraverso norme tecniche, elaborate da organismi internazionali di standardizzazione (come ISO, NIST, CEN e CENLEC), che hanno fornito un quadro concettuale di riferimento. L'espressione *Computer security* – e la sua successiva estensione, *Network security* – riflette la concezione originaria della

[5] Per una ampia ricostruzione degli attacchi informatici più rilevanti per la sicurezza nazionale e la stabilità internazionale, tra cui l'attacco a siti web di banche enti locali e testate giornalistiche in Estonia nel 2007, i primi casi di impieghi di armi cibernetiche nel conflitto Russo-Georgiano del 2008 e a quello Russo-Ucraino nel Donbas industriale del 2014, l'attacco ai sistemi di controllo SCADA da parte del *worm* Stuxnet per il sabotaggio di impianti iraniani di arricchimento dell'uranio si veda tra tutti G. D'ANGELO-G. GIACOMELLO, *Cybersicurezza. Che cos'è e come funziona*, Bologna, Il Mulino, 2023, p 165 ss. Si veda anche N. PERLROTH, *This Is How They Tell Me the World Ends: The Cyber Weapons Arms Race*, Bloomsbury, London, 2021.

[6] Per una descrizione di queste minacce e altri termini tecnici si può fare riferimento al Glossario della Agenzia Nazionale di Cybersicurezza consultabile all'indirizzo www.acn.gov.it/portale/csirt-italia/glossario. In particolare, *Denial of Service* è un attacco informatico che mira a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. Nella versione distribuita (DDoS) l'attacco proviene da un gran numero di dispositivi ed è diretto verso un target. *Spyware*, *trojan* e *rootkit* sono software, perlopiù malevoli, che permettono ad un attore ostile di accedere abusivamente ad un sistema informatico o a parte di esso, eludendo le protezioni di sicurezza e celando la propria presenza in modo tale da persistere nel corso del tempo con l'intento di raccogliere dati di varia natura (password, PIN, numero di carta di credito, dati di navigazione, ecc.) da computer e dispositivi e di trasmetterli successivamente a terze parti interessate al loro sfruttamento.

sicurezza informatica, intesa principalmente come protezione dell'elaboratore elettronico o, in senso più ampio, dell'intero sistema informatico, comprensivo di apparati hardware, software, infrastrutture e dei dati elaborati o trasmessi. Con l'evolversi della società verso modelli fortemente basati sulla produzione, circolazione e valorizzazione dell'informazione si è progressivamente affermata una nozione di sicurezza più ampia, orientata alla salvaguardia dell'informazione in quanto tale, sintetizzata nel concetto di *Information security*.

Pur nella varietà dei paradigmi che si sono succeduti nel tempo, una definizione ampiamente condivisa è stata introdotta dal NIST (*National Institute of Standards and Technology*) nella Special Publication 800-14, dove la sicurezza informatica è intesa come «la protezione fornita a un sistema informativo allo scopo di ottenere, come obiettivo applicabile, la conservazione dell'integrità, della disponibilità e della confidenzialità delle risorse del sistema informativo stesso (includendo hardware, software, firmware, dati e sistemi di telecomunicazione)». La definizione del NIST evidenzia l'orientamento sistemico della disciplina, che mira a garantire, in modo integrato attraverso l'adozione di politiche e misure tecniche, i principali requisiti della sicurezza – Riservatezza, Integrità e Disponibilità – ponendo le basi per la conformità a norme giuridiche e agli standard tecnici più diffusi, come la norma ISO/IEC 27001.

Accanto a questi tre requisiti cardine, cui gli esperti si riferiscono con l'acronimo RID (CIA, in inglese [7]), con il passaggio al paradigma dalla *Information security* sono stati introdotti ulteriori parametri finalizzati a garantire la certezza tecnica e giuridica delle relazioni digitali. Tra questi il principio del *non ripudio*, volto a impedire che un soggetto possa negare la paternità di una informazione; l'*autenticità* dell'informazione, che è la proprietà che un'entità (soggetto o risorsa) sia ciò che afferma di essere; la *verificabilità*, quale condizione indispensabile per consentire la tracciabilità e la trasparenza delle operazioni svolte nei sistemi informatici e infine l'*accountability* richiamata da diversi testi di legge comunitari, è la capacità di rendicontare con certezza e accuratezza le attività svolte da un'entità sul sistema [8]. Firme elettroniche, marche temporali, algoritmi di *hash*, fino ad architetture complesse come la blockchain, sono risposte specifiche a queste esigenze.

Le norme tecniche hanno assunto nell'ambito della cybersicurezza un ruolo di particolare rilievo, in quanto rappresentano l'espressione delle esigenze concrete provenienti dai principali attori privati e industriali del settore. Definendo

---

[7] La CIA triad è alla base di molteplici norme tecniche per la sicurezza informatica. Si veda, tra tutti, NIST (National Institute of Standards and Technology), Handbook on Computer security o anche UNI/EN ISO 27001.

[8] Si rimanda alle definizioni del NIST in M. NIELES *et al.*, *An Introduction to Information Security*, in *NIST Special Publication*, 800-12 Rev 1, 2017.

requisiti, metodologie operative e strumenti funzionali alla protezione dei sistemi informativi, hanno contribuito alla costruzione di un linguaggio tecnico condiviso. È noto, del resto, che il diritto ha progressivamente recepito gli standard tecnici, riconoscendone la centralità della sicurezza informatica nella regolazione degli ambienti digitali [9]. A partire dagli anni '90, la sicurezza informatica ha acquisito rilievo anche sul piano normativo, quando il legislatore ha introdotto specifiche fattispecie penali per l'accesso abusivo ai sistemi e la diffusione di malware, nonché standard minimi per le infrastrutture di telecomunicazione e obblighi di sicurezza nel trattamento dei dati personali.

Un passaggio chiave è rappresentato dalla Comunicazione della Commissione europea del 2001 dal titolo *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* [10], in cui si afferma che «la sicurezza sta diventando un tema di assoluta priorità perché le comunicazioni e le informazioni sono ormai fattori determinanti dello sviluppo economico e sociale». La Comunicazione sottolinea, in particolare, due aspetti fondamentali: da un lato, riconosce che la sicurezza dei sistemi informativi costituisce un presupposto essenziale per ogni ulteriore progresso tecnologico ed economico, conferendole dunque una valenza democratica e sistemica; dall'altro, propone una definizione di sicurezza informatica che, di fatto, ricalca gli standard tecnici allora già affermatisi a livello internazionale [11]. Vi si legge infatti che «sicurezza dei sistemi informatici e di rete» è la «capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema».

Già in tale sede, dunque, la Commissione europea riconduceva espressamente le misure in materia di sicurezza informatica a una cornice integrata di politiche pubbliche, che includevano la regolazione delle telecomunicazioni, la protezione dei dati personali e la prevenzione della criminalità informatica, anticipando così una visione olistica della cybersicurezza destinata ad assumere crescente centralità negli anni successivi.

---

[9] Si veda, in particolare, P. PERRI, *Sicurezza giuridica e sicurezza informatica dal d. lgs. n. 196/2003 al Regolamento generale sulla protezione dei dati*, in P. PERRI-G. ZICCARDI (a cura di), *Tecnologia e Diritto*, Giuffrè Francis Lefebvre, 2019, pp. 3-24; il capitolo dedicato alla Cybersicurezza in S. PIETROPAOLI, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, Giappichelli, 2023; P.G. CHIARA, *Il Diritto della Cybersicurezza*, in F. CASA (a cura di), *Intelligenza artificiale: diritto, etica e democrazia*, Bologna, Il Mulino, 2025, pp. 101-113; I. KAMARA, *Standardizing Personal Data Protection*, Oxford University Press, 2025.

[10] COM (2001)298.

[11] M. PIETRANGELO, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Riv. it. inf. e dir.*, 2024(2), pp. 13-24.

3. Elementi concettuali della sicurezza informatica

Le norme tecniche forniscono, fin dalle fasi preliminari della progettazione, principi di sicurezza di alto livello che costituiscono i pilastri della disciplina e si riflettono negli strumenti giuridici vigenti.

Ad un alto livello di astrazione la sicurezza informatica si estrinseca nello studio, progettazione e implementazione di strategie volte a proteggere la dimensione digitale da un pericolo (o dalla minaccia di un pericolo) di natura volontaria o accidentale. Le attività non si limitano all'adozione di strumenti tecnologici quanto, piuttosto, tendono alla definizione di politiche (norme, regole amministrative e procedure organizzative), alla predisposizione di meccanismi di controllo e alla promozione di comportamenti individuali corretti. Tra queste strategie rientrano procedure di autenticazione, gestione degli accessi, analisi dei rischi, aggiornamento dei sistemi, rilevazione e reazione ad incidenti o attacchi, recupero delle componenti oggetti di attacco, addestramento e formazione del personale [12].

La progettazione efficace della sicurezza – attraverso procedure, controlli, comportamenti e tecnologie – è guidata dal *controllo del rischio* [13]. La gestione del rischio permea tutta la disciplina della sicurezza informatica ed è alla base della più recente legislazione della UE in materia [14]. La regolazione e la gestione del rischio mirano a semplificare la complessità del contesto attraverso l'adozione di politiche, misure tecniche e modelli organizzativi in grado di contenere e mitigare le minacce individuate, perseguendo l'obiettivo generale di governare il rischio informatico. Il grado di esposizione al rischio, inteso come la probabilità di accadimento di un evento dannoso e l'entità delle sue conseguenze, diventa il parametro in base al quale determinare l'adozione di misure di sicurezza informatica conformi allo stato dell'arte e agli standard europei (ETSI, CEN) e internazionali (ISO/IEC) [15].

---

[12] Sia consentito il rimando a R. BRIGHI, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in TH. CASADEI-S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, Wolters Kluwer, 2024, pp. 75-87.

[13] Le norme tecniche internazionali (es. ISO 31000) definiscono il rischio come l'effetto dell'incertezza sugli obiettivi di sicurezza del sistema e stabiliscono metodologie e metriche per valutazione, analisi e gestione del rischio.

[14] A. MANTELERO *et al*., *The Common EU Approach to Personal Data and Cybersecurity Regulation*, in *International Journal of Law and Information Technology*, 4, 28, 2021, pp. 297-328; P.G. CHIARA-F. GALLI, *Normative Considerations on Impact Assessments in EU Digital Policy*, in *Media Law*, 1, 2024, pp. 86-105.

[15] I paradigmi normativi basati sul rischio, come GDPR, NIS, CSA, AIA e CRA, richiedono di contestualizzare i rischi, considerando non solo aspetti tecnici ma anche diritti fondamentali,

Le aree in cui si articolano le attività sono sostanzialmente tre: (i) realizzare sistemi robusti in grado di resistere agli attacchi, (ii) progettare metodi per il rilevamento di minacce ed anomalie al fine di garantire la resilienza dei sistemi; (iii) definire le risposte agli attacchi per ripristinare sistemi e servizi [16]. La robustezza impone che ogni componente del sistema sia progettata, configurata e mantenuta secondo criteri di protezione preventivi, fondati sull'esperienza storica dei rischi noti e sulle best practice del settore. Tuttavia, poiché le minacce evolvono rapidamente e possono manifestarsi in forme inedite, diventa indispensabile affiancare alla prevenzione tradizionale un approccio resiliente, in grado di adattare e riconfigurare il sistema durante l'evento avverso, garantendo così la continuità operativa e il ripristino di una nuova condizione di normalità. Infine, la dimensione della risposta si concretizza nella predisposizione di procedure e controlli volti a contenere immediatamente i danni, a mantenere le funzioni critiche e a organizzare il successivo recupero dei dati e il ripristino dell'intera infrastruttura. In tal modo, la disciplina della sicurezza informatica integra prevenzione, adattamento e reazione, offrendo un quadro metodologico coerente con le esigenze tecniche e normative. Ciascuna area comprende una vasta gamma di soluzioni tecniche e misure organizzative.

Alcuni *framework* di riferimento per il settore forniscono un insieme di linee guida, standard e *best practice*, richiamate anche dal quadro normativo in materia, che aiutano le organizzazioni a uniformare le pratiche di sicurezza e facilitano comunicazione e cooperazione. Tra tutti, è rilevante per la presente analisi il modello NIST [17] perché, oltre a essere molto noto nella comunità scientifica, è alla base del *Framework Nazionale per la Cybersecurity e la Protezione dei Dati* [18] e della tassonomia adottata dal decreto attuativo del Perimetro Nazionale di Sicurezza Cibernetica (PSNC), d.p.c.m. 14 aprile 2021, n. 81 in materia di notifiche degli incidenti e misure di sicurezza.

---

impatti sociali, legali, ambientali e sulla salute. Le misure di sicurezza e gli obblighi di segnalazione devono essere proporzionati all'esposizione ai rischi, alle dimensioni dell'ente e alla probabilità e gravità degli incidenti, conformi agli standard europei e internazionali. L'analisi dei rischi guida anche la scelta dei quadri di certificazione e dei livelli di garanzia, graduando gli obblighi di conformità secondo il grado di rischio. Tuttavia, le disposizioni astratte devono essere adattate al caso concreto dall'operatore, poiché i modelli tecnici di quantificazione risultano spesso inadeguati a misurare impatti complessi, come quelli sui diritti fondamentali, e i diversi quadri giuridici richiedono perimetri di rischio differenziati. P.G. CHIARA, *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, in *European Journal of Risk Regulation*, 2025, 16, pp. 1-16.

[16] M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds and Machines*, 2019, 29, p. 350.

[17] NIST (National Institute of Standards and Technology), Framework, https://www.nist.gov/cyberframework.

[18] CINI, Cyber Security National Lab, 2019, https://www.cybersecurityframework.it.

Data l'eterogeneità delle soluzioni, introdurre una tassonomia uniforme, accettata e consolidata è utile per tracciare una visione sistematica delle strategie di cybersicurezza.

La tassonomia del NIST definisce cinque funzioni chiave per il processo di gestione della cybersicurezza nel tempo: identificazione, protezione, rilevamento, risposta e ripristino. La fase di *identificazione* si concentra sull'individuazione delle criticità e dei rischi associati a sistemi, dati, asset e persone, fornendo le basi per le successive fasi di gestione. La *protezione* si occupa di implementare controlli adeguati a prevenire o contenere l'impatto di eventi negativi e attiene alla robustezza del sistema. La *rilevazione* è dedicata all'identificazione tempestiva di incidenti di sicurezza attraverso il monitoraggio continuo e l'analisi delle anomalie. La *risposta* prevede le attività necessarie per intervenire quando un incidente viene rilevato, con l'obiettivo di contenerne l'impatto. Infine, il *ripristino* riguarda la gestione dei piani per recuperare rapidamente la funzionalità dei processi e dei servizi colpiti da un incidente, garantendo la resilienza delle infrastrutture. Per ogni funzione chiave si sono sviluppate e riprese metodologie consolidate, strumenti tecnologici, raccomandazioni e strategie organizzative che includono, qualora il contesto lo richieda, anche i vincoli legali.

4. Cybersicurezza come sicurezza del Cyberspazio e nel Cyberspazio

A partire dall'impianto metodologico della cybersicurezza delineato negli standard tecnici, è emersa la necessità di ridefinirne la prospettiva originaria in quanto la pervasività delle tecnologie digitali e la loro integrazione trasversale in tutti i settori della società hanno trasformato profondamente il contesto operativo e hanno ampliato in modo significativo il perimetro da proteggere.

Ogni dimensione ed ambito della società contemporanea – dalla sanità all'istruzione, dal lavoro all'economia, fino alle istituzioni democratiche – è sostenuta da un'infrastruttura digitale in rapida e continua trasformazione. La cyber (in)sicurezza, non è più un problema settoriale o tecnico, limitato all'ambito delle tecnologie dell'informazione e della telecomunicazione (ICT), ma rappresenta oggi un rischio sistemico che incide trasversalmente su tutti i settori della vita sociale, economica e politica, con impatti profondi e duraturi. Nonostante la crescente digitalizzazione permane tuttavia un evidente divario tra il ritmo di adozione delle tecnologie e la capacità di raggiungere una protezione anche solo di base [19].

[19] Si vedano, tra tutti, ENISA, Threat Landscape, 2025; Relazione annuale (2024) al Parlamento della Agenzia per la Cybersicurezza nazionale; Rapporto Clusit 2025 sulla sicurezza ICT.

Secondo il Rapporto Clusit 2025, che analizza gli incidenti cyber più gravi avvenuti nel periodo di riferimento (nel caso di specie, 2024) su scala globale, il numero di attacchi informatici ha continuato a crescere in modo costante e allarmante [20]. Non è solo la frequenza degli attacchi ad aumentare, anche la gravità media degli incidenti si è accentuata costantemente, a causa di molteplici fattori, quali l'accelerazione della transizione digitale imposta dalla pandemia, l'intensificarsi delle tensioni geopolitiche che hanno alimentato una vera e propria guerra cibernetica diffusa e la rapidissima espansione dell'intelligenza artificiale.

Un cambiamento radicale nel panorama delle minacce coincide con lo sviluppo degli ambienti cyberfisici (CPS), reso possibile da tecnologie come il Cloud Computing e il 5G, e dall'integrazione pervasiva dell'IA [21]. I sistemi cyberfisici, nello specifico, si collocano all'incrocio tra il mondo fisico e quello digitale, integrando componenti quali oggetti fisici, software e reti per controllare i processi fisici in tempo reale. L'interconnessione continua con il mondo fisico implica un passaggio critico da sicurezza intesa come *security* a sicurezza intesa anche come *safety* [22], cioè quella dimensione volta a proteggere l'integrità della vita dalla minaccia di un pericolo imminente [23].

Se la pandemia ha evidenziato la funzione abilitante della cybersecurity come prerequisito strutturale della trasformazione digitale, le recenti tensioni geopolitiche hanno rivelato l'intrinseca fragilità degli spazi digitali e l'inevitabile interdipendenza tra sicurezza cibernetica, sovranità tecnologica e stabilità politica [24].

---

[20] Negli ultimi cinque anni, la media mensile degli incidenti confermati è quasi raddoppiata, passando da 156 nel 2020 a 295 nel 2024. Solo nel 2024, si è registrato un aumento del 27,4% rispetto all'anno precedente, con 3.541 attacchi noti, contro i 2.779 del 2023. Il Rapporto Clusit è liberamente scaricabile all'indirizzo: https://clusit.it/rapporto-clusit/.

[21] Tra i rischi individuati da ENISA nel rapporto previsionale *Foresight Cybersecurity Threats for 2030* la manipolazione intenzionale degli algoritmi e dei dati di addestramento della IA, l'abuso dei sistemi intelligenti, la compromissione della supply chain digitale e l'esposizione sistemica generata dai dispositivi IoT.

[22] A. VEDDER, *Safety, security and ethics*, in A. VEDDER *et al*. (a cura di), *Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Cambridge, Antwerp-Chicago, Intersentia, 2019, pp. 11-26.

[23] M. DURANTE, *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*, in D. BERKICH-M.V. D'AFONSO (a cura di), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence*, Springer Nature, 2019, p. 372.

[24] Il Rapporto di Europol *Internet Organised Crime Assessment* (IOCTA) 2023 evidenzia che gli effetti di trascinamento della situazione geopolitica si sono manifestati con una raffica di attacchi informatici dirompenti non solo contro obiettivi ucraini e russi, ma anche a livello mondiale, soprattutto nell'UE. Sul tema del cyberspazio come territorio di potenziali conquiste e – conseguentemente – conflitti tra gli Stati si veda L. MARTINO, *La quinta dimensione della*

Il rischio *cyber* non può più essere considerato un problema settoriale o meramente tecnico, bensì è una minaccia sistemica e multidimensionale, con implicazioni che travalicano i confini nazionali e investono direttamente la tenuta degli assetti democratici. Gli attacchi informatici di nuova generazione – più aggressivi, persistenti e sofisticati – sono vettori di instabilità: diffondono campagne di disinformazione, sostengono attività economiche illecite, alimentano conflitti tra Stati, rafforzano i meccanismi di controllo sociale e contribuiscono alla concentrazione del potere digitale, erodendo progressivamente le garanzie costituzionali e i principi dello Stato di diritto. Tali minacce, in grado di colpire sia gli interessi dello Stato che la fruibilità dei diritti dei soggetti di un ordinamento [25], hanno ridefinito natura e confini dello stesso concetto di sicurezza pubblica [26].

5. Cybersicurezza o Cyber sicurezza? Le definizioni degli organismi internazionali di standardizzazione

Di fronte a un ambiente sociotecnico interconnesso e dinamico, è ormai evidente che l'obiettivo del "rischio zero" è irrealizzabile; la complessità dei sistemi digitali e l'imprevedibilità delle minacce impongono un cambio di paradigma. È in questo contesto che si è progressivamente affermato il concetto di "cybersicurezza", quale espressione di un approccio più ampio e integrato. Esso va ben oltre la dimensione puramente tecnica della sicurezza informatica, per inglobare considerazioni di ordine strategico, politico, economico e giuridico.

---

conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale, in *Pol e soc*., n. 1/2018, p. 65 ss.; J. ERIKSSON-G. GIACOMELLO, *Cyberspace in Space: Fragmentation, Vulnerability, and Uncertainty*, in J. ERIKSSON (ed.), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, London and New York, Routledge, 2022, pp. 95-107; M. SMEETS, *Ransom War. How Cyber Crime Became a Threat to National Security*, C Hurst & Co Publishers Ltd, 2025. Per un approfondimento si rinvia ai contributi di G. GABRIELLI, *La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello jus ad bellum* e di R. ALLEGRI-G. SCICHILONE, *Il dominio cyber negli attuali scenari di guerra mediterranei: il caso del conflitto in Medio Oriente*, in questo volume.

[25] G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 4, p.76.

[26] Sul punto si vedano T.F. GIUPPONI, *Sicurezza e potere*, in *Enciclopedia del diritto*, *I tematici*, V, p. 1146 ss.; G. DE VERGOTTINI, *op. cit.*, p. 65 ss.; R. URSI, *La sicurezza cibernetica come funzione pubblica*, in R. URSI (a cura di), *La sicurezza nel cyberspazio*, p. 13 ss.; T.F. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, n. 2, 2024, pp. 180-181.

Come evidenziato dalla letteratura scientifica – ad esempio nello studio di Veale e Brown [27] – l'uso del termine *cybersecurity* implica un'espansione semantica e normativa del perimetro da proteggere. Non si tratta più solo di salvaguardare le reti e i sistemi informativi, ma di riconoscere l'interconnessione tra infrastrutture digitali, valori costituzionali, sicurezza nazionale e coesione sociale. Il rischio informatico, quindi, non è solo un fatto individuale ma, in determinate condizioni, una questione di interesse collettivo e pubblico, che può compromettere tanto i diritti dei singoli quanto la stabilità degli ordinamenti giuridici.

Il concetto di cybersecurity si configura quindi come significativamente più ampio rispetto a quello originario di *computer security* o *network security*, in quanto non si limita alla protezione tecnica delle reti, dei sistemi informativi e dei dati digitali, ma si estende alla salvaguardia dell'intero *cyberspazio*, inteso come ambito in cui interagiscono infrastrutture digitali, individui, organizzazioni e processi.

Tuttavia, tale ampliamento semantico solleva interrogativi di natura teorica e operativa, relativi alla definizione del cyberspazio, alla delimitazione del suo perimetro, all'individuazione degli elementi che lo compongono e dei beni che vi rientrano [28]. L'ambiguità definitoria si riflette nella delimitazione del campo d'azione della cybersecurity, in relazione (i) alla natura delle minacce da essa affrontate (solo quelle che hanno origini nel cyberspazio?), (ii) alla portata semantica del termine *cyber* – se riferito unicamente alla provenienza digitale delle minacce o anche a una specifica tipologia di beni da proteggere – e (iii) all'inclusione o meno, nel suo ambito, della protezione di asset fisici non concepiti primariamente per operare nel cyberspazio, ma ad esso connessi.

L'evoluzione verso sistemi cyberfisici (CPS) con la sua penetrazione trasversale in ambiti pubblici (es. infrastrutture critiche) e privati (es. industria 4.0 e ambienti domestici), ridefinisce la relazione tra cyberspazio e ambiente fisico, e impone un approccio olistico alla gestione del rischio [29]. Ogni attacco a sistemi CPS ha conseguenze su tutti gli oggetti fisici (inter) connessi e potenzialmente

---

[27] I dati riportati da Vale e Brown evidenziano che dal 2003 si fa sempre più riferimento a questo concetto sia nelle pubblicazioni accademiche che in quelle tradizionali, in campi che includono l'ingegneria del software, le relazioni internazionali, la gestione delle crisi e la sicurezza pubblica, superando lentamente termini più tecnici come computer security, system security o data security (diffuso negli anni '70/'80) e information security (diffuso dalla metà degli anni '90). M. VEALE-I. BROWN, *Cybersecurity*, in *Internet Policy Review*, n. 9, vol. 4, 2020.

[28] E. LONGO, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna Parlamentare*, 2, 2024, pp. 313-321.

[29] P.G. CHIARA, *The Internet of Things and EU Law: Cybersecurity, Privacy and Data Protection Challenges*, Cham, Springer, 2024.

un impatto diretto sulla vita delle persone [30]. La protezione, in questo quadro, deve riguardare simultaneamente la dimensione digitale, quella fisica e quella sociale.

È per questa ragione che, a differenza dei concetti tradizionali più tecnici, non esiste una definizione univoca e universalmente condivisa di *cybersecurity*: il termine si presta a una continua riconfigurazione, a seconda dei valori da proteggere, delle minacce emergenti e delle specificità dei contesti normativi.

In tal senso l'analisi delle definizioni adottate dagli organismi di standardizzazione internazionali evidenzia una notevole eterogeneità concettuale, strettamente correlata agli obiettivi e al contesto operativo delle istituzioni che le formulano [31]. Il *National Institute of Standards and Technology* (NIST), ad esempio, adotta una definizione focalizzata sulla componente intenzionale della minaccia, definendo la cybersecurity come la «capacità di proteggere o difendere l'uso del cyberspazio da attacchi informatici», con un accento esplicito sull'origine dolosa delle violazioni. Diversamente, le organizzazioni europee di standardizzazione – in particolare CEN e CENELEC – propongono un'accezione più articolata, secondo cui la cybersecurity riguarda la "sicurezza del cyberspazio", definito come «l'insieme dei collegamenti e delle relazioni tra oggetti accessibili attraverso una rete di telecomunicazioni generalizzata, nonché degli oggetti stessi, qualora dotati di interfacce che ne consentano il controllo remoto, l'accesso ai dati o l'interazione con altri dispositivi e sistemi». In questa prospettiva, l'elemento relazionale, la connettività e l'interoperabilità dei sistemi giocano un ruolo centrale nella definizione del dominio.

L'ontologia di *cybersecurity*, elaborata da ENISA insieme ai gruppi tecnici congiunti di CEN e CENLEC attraverso una ricognizione sistematica delle definizioni degli stakeholder, ben sintetizza la variabilità nella formalizzazione dei concetti chiave e dei principali componenti semantici del dominio: asset, minacce, attori, vulnerabilità, capacità difensive e impatti (Figura 1) [32].

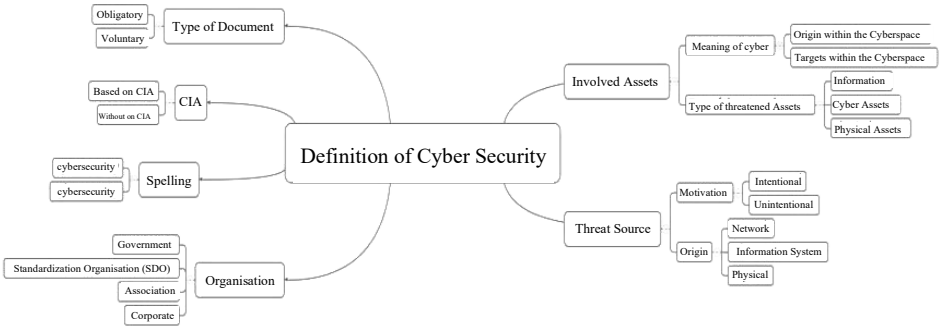
---

[30] L'"Internet of Medical Things" (IoMT) è un esempio significativo di come la cybersecurity stia progressivamente integrando considerazioni legate alla safety, poiché le tecnologie di cybersicurezza devono garantire l'integrità della vita contro gli attacchi informatici. S. KSIBI *et al.*, *A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach*, in *Mob. Netw Appl*., 2022 Sep 29, pp. 1-21.

[31] L.A. BYGRAVE, *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes*, in *Computer Law & Security Review*, 56, 2025, p. 5.

[32] ENISA, *Definition of Cybersecurity – Gaps and overlaps in standardisation*, v. 10, 2015.

Figura 1. – *Componenti che costituiscono il concetto di Cybersecurity* [33]



In definitiva, "Cybersicurezza" si presenta come un termine avvolgente, la cui definizione non può essere univoca né universalmente valida, poiché dipende dal contesto istituzionale, tecnico e politico in cui viene utilizzata.

Essa racchiude una molteplicità di significati e funzioni, riflettendo una crescente complessità nella natura delle minacce, nella varietà dei soggetti coinvolti e nell'eterogeneità dei valori da proteggere. Le definizioni adottate nei documenti normativi e tecnici risultano pertanto funzionali, piuttosto che ontologiche: servono a orientare le pratiche di sicurezza in relazione agli scopi e alle priorità dell'organizzazione che le impiega, piuttosto che a cristallizzare una nozione stabile e definitiva.

6. Concettualizzazioni di cybersicurezza nel diritto: il quadro attuale

A contribuire a una nuova concettualizzazione della cybersicurezza è l'approccio che l'Unione europea ha messo in atto a partire dal 2013, nell'emanazione di tre diverse *Cybersecurity Strategy* che promuovono una visione globale, basata sulla cooperazione internazionale, la condivisione di informazioni e la redistribuzione di responsabilità tra settore pubblico e privato [34]. In questo quadro, sono stati adottati o proposti diversi atti giuridici che lungo tre macroaree di intervento – la resilienza, il contrasto al cybercrimine, la cyberdifesa e la cyberdiplomazia – definiscono un nuovo assetto normativo in materia di

[33] ENISA, *Definition of Cybersecurity*, cit., p. 13.

[34] Commissione europea e alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza JOIN(2013) 1 final; JOIN(2017) 450 final; JOIN(2020) 18 final.

cybersecurity [35]. In Italia, la creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) nel 2021, all'interno del Piano Nazionale di Ripresa e Resilienza (PNRR), rappresenta un passo significativo verso un sistema di sicurezza più coordinato e robusto [36].

Mentre la Strategia del 2013 e gli atti che ne sono derivati, nel definire la cybersicurezza, richiamano esclusivamente la prospettiva tecnica «cibersicurezza si riferisce comunemente alle precauzioni e agli interventi che si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti», con l'emanazione del *Cybersecurity Act* (Reg. UE 2019/881) avviene un passaggio fondamentale che introduce una definizione più ampia e innovativa.

Secondo il *Cybersecurity Act*, la cybersicurezza deve includere «tutte le attività necessarie per proteggere i sistemi di rete e di informazione, gli utenti di tali sistemi e le altre persone interessate dalle minacce informatiche». Essa non si limita alla protezione dei sistemi e degli utenti, ma si estende anche a soggetti che, pur non essendo attori diretti, possono subire conseguenze dannose da minacce informatiche. In tal modo, la cybersicurezza si apre alla "sicurezza dell'umano" [37], andando oltre la mera tutela del business per includere la protezione della persona fisica e del bene pubblico [38].

In tale prospettiva, la cybersicurezza si articola in una struttura stratificata, che comprende dimensioni fisiche (hardware, cavi, router), logiche (software, protocolli) e sociali/semantiche (utenti e dinamiche umane). Questa visione multilivello è coerente con l'approccio multirischio illustrato in par. 3, che tiene conto non solo della sicurezza tecnica e fisica, ma anche di fattori non strettamente tecnologici, richiedendo una contestualizzazione del rischio e la promozione di misure preventive.

Si afferma così una concezione della cybersicurezza come strumento di tutela collettiva, connesso alle finalità proprie della sicurezza pubblica, quali la salvaguardia degli interessi nazionali, la stabilità delle istituzioni democratiche

---

[35] Per l'approfondimento dell'evoluzione del quadro normativo dell'Unione europea si rimanda al contributo di F. Casolari, F. Ferri e S. Villani in questo volume.

[36] L'Agenzia, che è il cardine della infrastruttura italiana di cybersecurity, è stata istituita con il d.l. n. 82/2021 e organizzata con il d.p.c.m. n. 223/2021.

[37] Così M.A. RIZZI-F.SERINI, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Riv. it. inf. e dir.*, 2024, p. 2.

[38] In argomento, V. TADDEO, *Is Cybersecurity a Pubblic Good*, cit.; R. BRIGHI-P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *Federalismi.it*, 21, 2021, pp. 18-42; P.G. CHIARA, *Una svolta nel dibattito sulla crittografia: la sentenza Podchasov c. Russia della Corte EDU. Verso alcuni diritti di cybersicurezza?*, in *Diritto & Questioni Pubbliche*, 2025, XXV, pp. 43-59.

e, più in generale, la promozione dell'ordinato vivere civile [39] in cui assumono particolare rilievo le azioni di cyberresilienza tecnico-economica e la diffusione capillare di una cultura della sicurezza informatica.

Parallelamente a tale visione sociale e pubblicistica, continua a dispiegarsi una dimensione tecnico-economica della cybersicurezza, incentrata su un approccio operativo e funzionale [40].

In questo ambito, la cybersicurezza è trattata come un insieme di obblighi normativi volti a garantire l'adeguatezza delle misure tecniche di protezione, la tempestiva comunicazione di eventuali incidenti alle autorità competenti e il rispetto di standard minimi comuni per la certificazione del livello di sicurezza di beni e servizi immessi sul mercato. Si delinea così un modello tecnicistico e verticale, che comporta l'introduzione di nuovi obblighi regolatori [41].

Tale modello, pur nella sua complessità procedurale, rappresenta una dimensione imprescindibile in un settore fortemente specializzato. Esso incentiva la cooperazione tra settore pubblico e privato nella definizione dei requisiti tecnici, nella creazione di meccanismi di fiducia e nella promozione di soluzioni di sicurezza by design.

Il diritto, in questo contesto, interviene dettando requisiti minimi e standard normativi, mentre le certificazioni svolgono una funzione di garanzia, orientando i produttori e rafforzando la fiducia dei cittadini nei confronti dei servizi digitali.

Gli attacchi informatici non possono più essere considerati mere questioni tecniche, ma si configurano come temi di interesse pubblico, rispetto ai quali il diritto è chiamato a rispondere con strumenti adeguati, multilivello e multidisciplinari. Questo ampliamento riflette non solo l'impatto trasversale degli incidenti informatici sulla sicurezza collettiva, ma anche la crescente interdipendenza tra spazio cibernetico e sistema socio-istituzionale. La cybersicurezza, dunque, si configura oggi come un elemento strutturale e fondativo dell'ecosistema digitale globale.

---

[39] Così M. PIETRANGELO, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, cit., p. 16. Si veda anche R. URSI, *La sicurezza pubblica*, il Mulino, 2022.

[40] Sul punto, in particolare, si vedano i contribuiti della *Parte 2 – Cybersicurezza e protezione degli eco-sistemi cyberfisici: una visione strumentale* di questo volume.

[41] Carichi regolatori che gravano in particolare su imprese e start-up che operano nei settori innovativi. EUROPEAN COMMISSION, *The future of European competitiveness*, September 2024. Per l'esame della regolazione dell'Unione europea sulla cybersicurezza, in particolare del Cyber Resilience Act, nella prospettiva del diritto del commercio internazionale e dunque degli impatti sugli scambi internazionali, si veda il contributo di A. ADINOLFI-R. MAGNAGHI, *Il Cyber Resilient Act nella prospettiva degli accordi commerciali dell'Unione europea*, in questo volume.

7. Conclusione

La cybersicurezza va interpretata come un concetto articolato e in continua evoluzione, suscettibile di molteplici declinazioni semantiche. Non è più possibile circoscrivere il termine entro una definizione statica, capace di rappresentare esaustivamente l'insieme degli asset da tutelare, le tipologie di rischio cui far fronte e la molteplicità degli attori (istituzionali, economici e civili) coinvolti. Piuttosto dall'insieme delle prospettive analizzate prende forma un modello olistico, capace di abbracciare le diverse dimensioni e i molteplici livelli di interazione all'interno di società interamente dipendenti dal digitale. Non si tratta solo di rafforzare strumenti di difesa tecnologica, ma di costruire un ecosistema di sicurezza che integri politiche pubbliche, pratiche sociali, processi formativi diffusi e responsabilità condivise.

Un modello olistico di cybersicurezza poggia su diversi pilastri. Innanzitutto, serve un'architettura normativa coerente che renda chiari gli obblighi regolamentari e rafforzi il principio di certezza del diritto [42]. Parallelamente è fondamentale incorporare meccanismi di governance del rischio "by design" [43], ovvero progettare i sistemi con criteri di sicurezza fin dalle origini. In termini operativi ciò significa integrare misure di prevenzione, rilevazione e resilienza in tutto il ciclo di vita delle tecnologie, con il supporto di processi di certificazione e standardizzazione [44]. Infine, il terzo pilastro è l'impegno attivo delle comunità, attraverso la promozione di percorsi educativi territoriali e di iniziative di monitoraggio partecipato, volti a consolidare una cultura condivisa della sicurezza

---

[42] A. BYGRAVE, *cit*.

[43] L.A. BYGRAVE, *Security by Design: Aspirations and Realities in a Regulatory*, in *Oslo Law Review*, 2021, 8; nel contesto della 'vicina' area della protezione dei dati personali, si veda *ex multis* G. BINCOLETTO, *Data Protection by Design in the E-Health Care Sector*, Nomos, 2021.

[44] Le metodologie e gli strumenti propri dell'informatica giuridica si prestano ad essere utilizzati per rendere operative normative caratterizzate da elevata complessità tecnico-giuridica. In tale prospettiva, uno degli esiti del progetto EcoCyber consiste nella realizzazione di una guida interattiva e di agevole consultazione dedicata al Cyber Resilience Act (Regolamento UE 2024/2847). Attraverso l'utilizzo del *legal design*, una metodologia interdisciplinare che integra competenze giuridiche, comunicative e visive, le disposizioni normative vengono tradotte in strumenti chiari, visuali e pratici, destinati a tutti i portatori di interesse: dai produttori di tecnologie, ai ricercatori, fino agli esperti di cybersecurity e agli utenti finali. Alle basi vi è una mappatura completa dei contenuti su più livelli, in chiave tecnica e in chiave giuridica, così da poterli rianalizzare a fondo e ricostruire un'architettura logica chiara e coerente. Cfr. *Whitepaper on the EU Cyber Resilience Act: what it is, how it works, and how it can be operationalised. A legal design approach*, P.G. Chiara, A. Vannini, I. Morciano, R. Brighi, M. Prandini.

digitale [45]. Su questa necessità insiste tanto la citata Strategia europea quanto la Strategia nazionale di cybersicurezza del nostro Paese che prevede interventi formativi a tutti i livelli: dai programmi scolastici e universitari alla formazione nelle pubbliche amministrazioni, fino allo sviluppo di un sistema di certificazione nazionale per valutare le conoscenze e le competenze in materia di cybersecurity e uno strumento di formazione e sensibilizzazione online rivolto al grande pubblico per l'autoverifica delle competenze acquisite [46].

Questo approccio integrato si traduce in una cooperazione rafforzata tra settore pubblico e privato, nell'attivazione di interventi educativi a livello territoriale e il sostegno alle piccole e medie imprese attraverso misure amministrative adeguate. Fondamentale, inoltre, è incentivare forme di partecipazione civica e azioni di monitoraggio sociale, riconoscendo il valore delle iniziative collettive come componente integrante delle politiche di sicurezza. In definitiva, la cybersicurezza può dirsi effettiva solo se è plurale, interconnessa e radicata nel tessuto sociale, andando oltre la mera logica normativa o tecnologica.

Guardando al futuro, le analisi accademiche e politiche dovranno focalizzarsi sulla valutazione empirica di questi modelli integrati. Al momento mancano indicatori di performance condivisi in grado di quantificare congiuntamente i risultati tecnologici, le ricadute normative e gli impatti socio-culturali. È pertanto auspicabile un approccio di ricerca sistemico e multidisciplinare che sviluppi metriche articolate per disegnare politiche di cybersicurezza veramente sostenibili e resilienti, calibrate su evidenze concrete e sull'osservazione reale dei fenomeni.

---

[45] Molteplici iniziative di formazione e educazione sono esito del paternariato SERICS. Si veda tra tutti, il progetto SAFLEY – *Social media Awareness For Education and Legal Youth* (www.safely.unimore.it), sviluppato nello Spoke 8 (Gestione del rischio e governance) con il coordinamento dell'Università di Modena e Reggio Emilia, all'interno del CRID – Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità. Il progetto ha dato vita ad un laboratorio multidisciplinare dedicato alla promozione di una cittadinanza digitale critica, consapevole e inclusiva, che mediante incontri, seminari, attività laboratoriali. TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *GIOVANI IN RETE. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025.

[46] Come approfondimento si rimanda ai contributi di A. CARBONARO-E. GNAGNARELLA, *Cybersicurezza e fattore umano: un approccio educativo inclusivo* e di V. BARONE-TH. CASADEI, *Per un uso consapevole e sicuro delle tecnologie: strategie educative e misure di intervento*, in questo volume.

Capitolo 2

La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea

Federico Casolari [*], Federico Ferri [**], Susanna Villani [***]

Abstract: Il contributo dà conto del contesto nel quale hanno preso corpo le molteplici iniziative che oggi compongono il diritto UE della cybersicurezza, contesto che va inserito all'interno del più ampio processo di costituzionalizzazione dell'Unione. L'interesse per una simile disamina è duplice. Anzitutto, essa consente di mettere a sistema una normativa che si sta sviluppando in un modo per certi versi ipertrofico, consentendo all'operatore giuridico di meglio comprenderne il significato e l'orientamento teleologico. In secondo luogo, ciò consente anche di evidenziare le implicazioni costituzionali del processo in corso, che incidono tanto sull'allocazione delle competenze tra Stati membri e Unione europea quanto sulla qualità del *law making* sovranazionale.

Keywords: Autonomia strategica – Art. 2 TUE – Competenze dell'Unione europea – Sovranità digitale europea – Sicurezza nazionale e sicurezza sovranazionale – *Law making*

[*] Professore ordinario di Diritto dell'Unione europea, Direttore del Dipartimento di Scienze Giuridiche dell'Università di Bologna, federico.casolari@unibo.it.

[**] Ricercatore a tempo determinato di tipo B in Diritto dell'Unione europea, Dipartimento di Scienze Giuridiche dell'Università di Bologna, federico.ferri5@unibo.it.

[***] Ricercatrice a tempo determinato di tipo A in Diritto dell'Unione europea, Dipartimento di Scienze Giuridiche dell'Università di Bologna, susanna.villani2@unibo.it.

1. Cybersicurezza e autonomia strategica dell'Unione: una visione di insieme

"L'Europa è impegnata in una lotta. Una lotta per un continente integro che viva in pace, per un'Europa libera e indipendente. Una lotta per i nostri valori e le nostre democrazie, per la libertà e la capacità di scrivere da soli il nostro destino. Possiamo esserne certi: è una lotta per il nostro futuro" [1]. Sono queste le parole che Ursula von der Leyen ha utilizzato per aprire il suo discorso sullo stato dell'Unione 2025. Per quanto possano apparire enfatiche e, per certi versi, cariche di preoccupazione per il futuro, esse non arrivano inaspettate. Da tempo ormai il linguaggio – e lo strumentario – utilizzato dalle istituzioni sovranazionali si sta orientando nel senso di predisporre misure ed iniziative che mirino alla salvaguardia dei valori e degli interessi dell'Unione e dei suoi Stati membri rispetto a minacce esterne sempre meno prevedibili e convenzionali. È questa la dottrina c.d. dell'"autonomia strategica" dell'Unione [2], che risulta trasversale alle molteplici manifestazioni dell'agire sul piano sovranazionale. Un tale riorientamento strategico riguarda tanto la dimensione, per così dire, *offline* quanto quella *online* dell'azione UE. E, inevitabilmente, non può non riguardare il tema della cybersicurezza, che si pone per certi versi a cavaliere tra i due ambiti appena richiamati. Se ne ha un'evidente riprova nella *Strategia dell'UE in materia di cibersicurezza per il decennio digitale*, adottata nel 2020, che evidenzia la necessità di una visione olistica nella reazione alle minacce cibernetiche alla società europea [3]. A partire dalle minacce rispetto a ciò che si pone a fondamento di tale società [4] e che costituisce al contempo l'elemento identitario

[1] V. Discorso della Presidente von der Leyen sullo stato dell'Unione 2025, disponibile al link: https://ec.europa.eu/commission/presscorner/detail/it/SPEECH_25_2053.

[2] Su di essa, v., per tutti, N. HELWIG-V. SINKKONEN, *Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term*, in *European Foreign Affairs Review*, 2022, p. 1 ss.; F. HOFFMEISTER, *Strategic Autonomy in the European Union's External Relations Law*, in *Common Market Law Review*, 2023, p. 667 ss.

[3] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020) 18 final.

[4] Su quest'ultimo concetto, v. A. VON BOGDANDY, *The Emergence of European Society*

dell'ordinamento giuridico sovranazionale [5], vale a dire la base valoriale su cui poggia l'Unione europea *ex* art. 2 TUE. In questo senso, le traiettorie dell'autonomia strategica intercettano quelle del quadro costituzionale dell'Unione, collocando all'interno di quest'ultimo le numerose iniziative che sono state adottate sino ad ora per promuovere la cybersicurezza sovranazionale.

Questo contributo non intende fornire una ricostruzione dettagliata e articolata di tali iniziative. Lo scopo è semmai quello di dare conto del contesto in cui esse si pongono, contesto che va inserito, come appena detto, all'interno del più ampio processo di costituzionalizzazione dell'Unione. L'interesse per una simile disamina è duplice. Anzitutto, essa consente di mettere a sistema una normativa che si sta sviluppando in un modo per certi versi ipertrofico, consentendo all'operatore giuridico di meglio comprenderne il significato e l'orientamento teleologico. In secondo luogo, ciò consente anche di evidenziare le implicazioni costituzionali del processo in corso, che incidono tanto sull'allocazione delle competenze tra Stati membri e Unione europea quanto sulla qualità del *law making* sovranazionale [6].

2. Le competenze dell'Unione in materia di cybersicurezza

La proliferazione delle iniziative UE sulla cybersicurezza impone anzitutto una contestualizzazione della materia all'interno dei rapporti multilivello disciplinati da norme di diritto primario dell'Unione. In particolare, occorre indagare il riparto di competenze e poteri tra Unione e Stati membri alla luce delle basi giuridiche a disposizione del legislatore sovranazionale e della prassi emersa sino ad ora.

Va anzitutto fatto presente che l'Unione non sarebbe direttamente competente a intervenire nel campo della cybersicurezza intesa in senso stretto. In altre parole, il testo dei Trattati istitutivi non enuncia questa espressione, né contiene indicazioni specifiche per poterla ricondurre agli elenchi contenuti nelle principali disposizioni in punto di suddivisione di competenze, vale a dire gli artt. 3, 4 e 6 TFUE. Ne consegue che non è nemmeno stato inserito un titolo o un capo *ad hoc* nella Parte III del TFUE, nella quale figurano le politiche e azioni interne dell'Unione.

---

through Public Law. A Hegelian and Anti-Schmittian Approach, Oxford University Press, Oxford, 2024.

[5] Corte giust., C-156/21, *Ungheria c. Parlamento europeo e Consiglio*, 16 febbraio 2022, punto 127.

[6] Sebbene il capitolo nasca da riflessioni comuni e condivise, Federico Casolari è autore dei paragrafi 1 e 4, Federico Ferri del paragrafo 2 e Susanna Villani del paragrafo 3.

Le norme discusse in questo volume trovano la loro ragion d'essere in obiettivi raggiungibili mediante un'interpretazione (e, di riflesso, un'attuazione) elastica delle logiche sottese al principio di attribuzione e all'esercizio delle competenze. Stante l'evidente porosità dei confini che dovrebbero teoricamente separare le varie politiche dell'Unione [7], le istituzioni coinvolte nelle procedure di adozione degli atti legislativi hanno "occupato" progressivamente certi spazi, includendovi istanze e prerogative della cybersicurezza.

Il retroterra di riferimento è con tutta probabilità il Mercato Unico Digitale (MUD), oggetto per la prima volta di una strategia di ampio respiro nel 2015, quando fu pubblicata un'apposita comunicazione della Commissione europea [8]. Fermo restando che, come ampiamente noto, il MUD ad oggi viene concretizzato da una moltitudine di atti vincolanti di varia natura [9], è appena il caso di ricordare che la cybersicurezza è considerata un contenuto di un certo rilievo nell'economia di questo spazio a tratti "ubiquo" [10] e in continua evoluzione. È attraverso tale paradigma che saranno ricostruite a seguire alcune delle traiettorie più significative che si riferiscono alle competenze spendibili per la creazione di un diritto UE sulla cybersicurezza.

2.1. Il progressivo affrancamento dal pilastro intergovernativo e il rapido distanziamento dalla teoria dei poteri impliciti

In primo luogo, conviene, però, guardare alla cybersicurezza da un'altra angolatura, per sgombrare il campo da alcuni elementi che hanno accompagnato,

---

[7] Tra i tanti, R. ADAM-A. TIZZANO, *Manuale di Diritto dell'Unione europea*, Giappichelli, Torino, 2020, p. 430.

[8] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final.

[9] Per approfondimenti sull'estensione del MUD si veda, senza alcuna pretesa di esaustività: G. CAGGIANO, *Il quadro normativo del Mercato unico digitale*, in F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, Fascicolo speciale, 2020, p. 13 s.; S. GARBEN-I. GOVAERE (eds), *The Internal Market 2.0*, Hart Publishing, Oxford-New York, 2020; P. MANZINI-G. CONTALDI-G. CAGGIANO (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, Bari, 2021; T.-E. SYNODINOU-P. JOUGLEUX-C. MARKOU-T. PRASTITOU-MERDI (eds), *EU Internet Law in the Digital Single Market*, Springer, Cham, 2021; Ł.D. DĄBROWSKI-M. SUSKA (eds), *The European Union Digital Single Market: Europe's Digital Transformation*, Routledge, Oxon-New York, 2022; V. PAPAKONSTANTINOU-P. DE HERT, *The Regulation of Digital Technologies in the EU, Act-ification, GDPR Mimesis and EU Law Brutality at Play*, Routledge, Oxon-New York, 2024; W. KILIAN, *EU Digital Markets Law. A Concise Guide to the Regulations and Directives on IT and Media Law*, Edward Elgar, Cheltenham-Northampton, 2025.

[10] PARLAMENTO EUROPEO, *Ubiquità del mercato unico digitale*, https://www.europarl.europa.eu/factsheets/it/sheet/43/ubiquita-del-mercato-unico-digitale.

in via diretta o indiretta, il tema delle competenze nelle prime fasi di sviluppo del diritto sovranazionale *in subiecta materia*. Preme in particolare avanzare alcune rapide considerazioni a monte, e cioè sui retaggi del vecchio pilastro intergovernativo della celebre struttura eretta con il Trattato di Maastricht del 1992, nonché in ordine ai poteri che l'Unione potrebbe in certi casi esercitare pur in assenza di competenza.

Da un lato, pare utile rammentare che a lungo la normativa d'appoggio per ciò che oggi chiamiamo oggi "cybersicurezza" è stata una decisione quadro del Consiglio [11] adottata nel contesto dell'allora pilastro "Giustizia e affari interni" (GAI), che compendiava aree d'azione sottoposte a intensi poteri degli Stati membri. La decisione in parola fu poi sostituita nel 2013 dalla direttiva relativa agli attacchi contro i sistemi di informazione [12], avente per base giuridica l'art. 83, par. 1, TFUE, disposizione riconducibile all'alveo dell'originario pilastro GAI e che consente al legislatore dell'Unione di stabilire misure minime per la definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave e a dimensione transnazionale. Come si vede, si tratta di esempi ancora estranei alle logiche istituzionali del mercato interno e al raggio d'azione (invero molto vasto) di questa politica.

Per altro verso, nella predetta strategia sul MUD, che anticipò di poco tempo l'adozione della prima direttiva NIS [13], l'esigenza di interventi normativi sulla cybersicurezza è stata in buona parte riportata all'obiettivo concernente la protezione delle reti e infrastrutture critiche [14]. All'epoca questo settore era coperto solo in misura parziale dal diritto derivato: rilevava la direttiva 2008/114/CE [15], che si estendeva all'individuazione, designazione e protezione delle infrastrutture critiche europee. Sennonché, la base giuridica della direttiva sulle infrastrutture critiche europee era l'art. 308 del previgente Trattato sulla Comunità europea, ossia la norma che enunciava la cosiddetta "teoria dei poteri impliciti". Essa di fatto consentiva al Consiglio di intervenire anche in mancanza di poteri previsti allo scopo dal Trattato, purché la misura fosse adottata all'unanimità e

[11] Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione, GU L 69, 16 marzo 2005.

[12] Direttiva (UE) 2013/40 del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, GU L 218, 14 agosto 2013.

[13] 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, GU L 194, 19 luglio 2016.

[14] COM(2015) 192, p. 14.

[15] Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, GU L 345, 23 dicembre 2008.

a patto che l'azione da intraprendere si rivelasse necessaria per raggiungere uno degli scopi della Comunità, ancorché nel funzionamento del mercato comune [16]. Ancora una volta, a ben vedere, il modello regolatorio della cybersicurezza sembrava poter essere accostato a strumenti di limitata operatività, o per lo meno *sui generis*.

La realtà ad oggi è ben diversa, come dimostrano gli elementi di prassi susseguitisi col passare del tempo nell'ultimo decennio.

2.2. La dimensione interna: il ruolo predominante (ma non esclusivo) dell'art. 114 TFUE

Dal punto di vista materiale, il quadro giuridico di riferimento si allinea in una certa misura al *trend* che accomuna la delineazione di molti degli atti legislativi con i quali l'Unione sta cercando di dare corpo alla propria trasformazione digitale, e dunque anche al MUD. Tale allineamento è contrassegnato dalla sussunzione di più settori alla competenza dell'Unione in materia di mercato interno. Ciò vale, a mero titolo di esempio, per l'intelligenza artificiale, i servizi e i mercati digitali, solitamente i dati personali, e spesso anche la cybersicurezza. Rispetto a quest'ultima, l'ancoraggio al mercato interno è tipico di atti quali il *Cybersecurity Act* [17], la direttiva NIS 2 [18] (e, in precedenza, pure la NIS1) o il *Cyber Resilience Act* [19].

Chiarire questo aspetto è importante, dal momento che il mercato interno è una competenza UE di tipo concorrente e quindi suscettibile di assicurare all'Unione l'esercizio di forti poteri. Gli atti di cui sopra, non a caso, hanno per base giuridica l'art. 114 TFUE. Il primo paragrafo di questa disposizione permette all'Unione di adottare misure relative al ravvicinamento delle disposizioni

[16] Il Trattato di Lisbona enuncia ora la "clausola di flessibilità", all'art. 352 TFUE, che riprende molti contenuti dell'art. 308 TCE, ma non propone più il collegamento necessario al funzionamento del mercato interno.

[17] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), GU L 151, 7 giugno 2019.

[18] 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), GU L 333, 27 dicembre 2022.

[19] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza), GU L 2024/2847, 20 novembre 2024.

legislative, regolamentari ed amministrative degli Stati membri che abbiano per oggetto l'instaurazione ed il funzionamento del mercato interno. Si parla di atti legislativi di armonizzazione, indipendentemente dal margine di manovra di cui, nella sostanza del singolo caso, potranno effettivamente beneficiare i destinatari dei vari obblighi. Lo stesso dicasi anche per quegli atti che presentano una o più basi giuridiche aggiuntive accanto all'art. 114 TFUE, dal momento che solitamente è proprio questa disposizione a fungere da "centro di gravità" della misura, finendo dunque per acquisire un peso specifico superiore.

Si capisce che nel nuovo ecosistema giuridico elaborato per realizzare il MUD si sono rinvenute le condizioni per consolidare la posizione della cybersicurezza nel sistema UE delle competenze (dunque evitando di ricorrere alla versione aggiornata della teoria dei poteri impliciti) e per darle una collocazione sostanzialmente diversa rispetto ai primi esperimenti normativi, radicati, come detto poc'anzi, nel vecchio pilastro GAI, piuttosto che nell'odierna cooperazione giudiziaria in materia penale. La circostanza non pare sorprendente, anche alla luce di una giurisprudenza della Corte di giustizia che da decenni conferma l'ampia libertà di azione del legislatore dell'Unione allorché questi ritenga di dover armonizzare dati settori [20], consentendogli peraltro di giustificare agilmente il rispetto dei principi di sussidiarietà e proporzionalità *ex* art. 5, par. 3 e par. 4, TUE.

Più in generale, la scelta (senza alcuna opposizione, questo va sempre tenuto a mente) di riportare anche la cybersicurezza sotto l'ombrello dell'art. 114 TFUE esprime l'attitudine di questa disposizione ad essere utilizzata in senso ampio e con una certa disinvoltura, quasi come una sorta di "*passepartout*" [21], naturalmente in virtù del graduale ampliamento sostanziale e funzionale del concetto di mercato interno rispetto alle origini [22].

Ecco che allora l'art. 114 TFUE è stato utilizzato come base giuridica per il *Cybersecurity Act* sia per dare seguito alla pronuncia *Regno Unito c. Parlamento europeo e Consiglio* del 2006 [23], sia per superare la frammentazione dei

---

[20] V., ad esempio, Corte giust., C-491/01, *British American Tobacco e Imperial Tobacco Limited*, 10 dicembre 2002; C-58/08, *Vodafone Ltd e altri*, 8 giugno 2010.

[21] A tale proposito, si specifica che la predetta direttiva sulle infrastrutture critiche europee, basata sull'art. 308 TCE, è stata sostituita da una direttiva avente per base giuridica l'art. 114 TFUE: si tratta della Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, GU L 333, 27 dicembre 2022.

[22] Per spunti di riflessione e approfondimenti sul tema, si rinvia a S. WEATHERILL, *The Internal Market as a Legal Concept*, Oxford, Oxford University Press, 2016, C. BARNARD, *The Substantive Law of the EU: The Four Freedoms*, Oxford, Oxford University Press, 2022.

[23] Corte giust., C-217/04, *Regno Unito di Gran Bretagna e Irlanda del Nord c. Parlamento europeo e Consiglio dell'Unione europea*, 2 maggio 2006.

sistemi di certificazione per i prodotti e i servizi TIC. Diversamente, nel nuovo regime corrispondente alla direttiva NIS 2 la *ratio* dell'art. 114 TFUE è permettere al legislatore di stabilire norme chiare e generalmente applicabili a favore di soggetti ritenuti essenziali e importanti, oltre che di armonizzare le norme applicabili nel settore della gestione del rischio di cybersicurezza e della segnalazione di incidenti. Invece, il fondamento del *Cyber Resilience Act* sull'art. 114 TFUE risiede nel tentativo di dare una cornice più adeguata all'essenza transfrontaliera della cybersicurezza nei beni digitali, cosa che giustificherebbe la decisione di armonizzare i requisiti di cybersicurezza per i prodotti con elementi digitali in tutti gli Stati membri, specialmente in una prospettiva di rimozione degli ostacoli alla libera circolazione delle merci.

Le connotazioni caratterizzanti del contesto appena illustrato non paiono snaturarsi a causa della sussistenza di ulteriori misure sulla cybersicurezza che possiedono basi giuridiche diverse dall'art. 114 TFUE.

In effetti, se si considera il recente regolamento sulla cybersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione [24], si nota che il fondamento normativo è l'art. 298 TFUE, a difesa della garanzia di un'amministrazione europea aperta, efficace ed indipendente. Tuttavia, non sfugge di certo che la sfera applicativa di tale misura è estremamente limitata, almeno *ratione personae*.

Discorso relativamente diverso per il *Cyber Solidarity Act* [25], che al posto dell'art. 114 TFUE prevede come basi giuridiche gli artt. 173 e 322, par. 1, lett. a), TFUE. L'inserimento della seconda base giuridica, riguardante le regole finanziarie che stabiliscono in particolare le modalità relative alla formazione e all'esecuzione del bilancio, al rendiconto e alla verifica dei conti, deriva dalla presenza di diverse disposizioni tecniche che assicurino un certo grado di flessibilità in relazione alla gestione del bilancio. L'art. 173 TFUE è il baricentro reale dell'atto e si riferisce alla politica industriale dell'Unione. Contrariamente al mercato interno, questa politica è di mero sostegno o supporto e comprime fortemente i poteri di intervento dell'Unione, che non ha titolo per porre in essere obblighi di armonizzazione: diviene quindi prevalente il livello nazionale. Eppure, sono pacifiche le saldature del *Cyber Solidarity Act* al mercato interno, in quanto il regolamento, nel suo complesso, costituisce un passaggio mediato per favorire un aumento della competitività dell'Unione in tale area.

---

[24] 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, GU L 2023/2841, 18 dicembre 2023.

[25] Regolamento (UE) 2025/38 del Parlamento Europeo e del Consiglio del 19 dicembre 2024 che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà), GU L, 2025/38, 15 gennaio 2025.

2.3. *Segue*: la portata della riserva di competenza in tema di sicurezza nazionale a favore degli Stati membri

I rilievi sulle basi giuridiche "interne" degli atti legislativi che compongono il diritto UE sulla cybersicurezza si ramificano ulteriormente allorché ci si addentra nella sfera della sicurezza nazionale [26]. La questione di fondo è posta nel secondo comma dell'art. 4 TUE. Questa disposizione sancisce talune prerogative di prim'ordine a favore degli Stati membri e tra esse spicca, appunto, la sicurezza nazionale: non solo tale ambito è incluso nelle funzioni essenziali statali che l'Unione deve rispettare, ma l'ultimo enunciato dell'art. 4, par. 2, TUE aggiunge un rafforzativo speciale, stabilendo che "(i)n particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro". Significa che gli Stati membri, nella loro qualità di sovrani dei Trattati, avrebbero precluso all'Unione qualsivoglia possibilità di intervento in un settore che ritenevano talmente strategico da non poter prestare il fianco ad alcuna incursione da parte di altri ordinamenti giuridici.

Resta il fatto che l'esistenza di un sistema di atti legislativi UE per la cybersicurezza tende inevitabilmente a toccare questo nucleo teoricamente inaccessibile. Nonostante gli atti legislativi oggetto di questo capitolo ribadiscano i limiti introdotti dall'art. 4, par. 2, TUE, non si vede in che modo, all'atto pratico, sia possibile mantenere una separazione totale fra traiettorie d'intervento sovranazionali e nazionali. Come spiegare questo apparente cortocircuito?

Preliminarmente, ci si rifà a quella giurisprudenza della Corte di giustizia che offre una lettura meno granitica del testo dell'art. 4, par. 2, TUE. Fatta salva una fisiologica zona operativa nella quale ciascuno Stato membro è libero di agire in via esclusiva a tutela della propria sicurezza nazionale, per la Corte sussiste comunque un divieto in capo alle autorità nazionali competenti di attuare detta eccezione allo scopo di eludere obblighi di diritto UE [27]. Anche l'opinione di molti autori conferma che la linea di demarcazione tracciata dall'art. 4, par. 2, in fin dei conti è più mobile di quanto possa sembrare a prima vista [28].

---

[26] Si veda diffusamente anche il capitolo di T. F. GIUPPONI, *Il quadro della governance della cybersicurezza a livello nazionale*, in questo volume.

[27] Tra gli esempi più indicativi si segnala Corte giust., C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, 6 ottobre 2020, punto 99.

[28] Per maggiori dettagli, si rinvia B. DE WITTE, *Les compétences exclusives des états membres existent-elles?*, in AA.VV. (a cura di), Liber amicorum *per Antonio Tizzano*: de la Cour CECA à la Cour de l'Union: le long parcours de la justice Européenne, Giappichelli, Torino, 2018, p. 301 s.; G. DI FEDERICO, *L'identità nazionale degli Stati membri nel diritto dell'Unione europea: natura e portata dell'art. 4, par. 2, TUE*, Editoriale Scientifica, Napoli, 2017, p. 156 s.; F. FERRARO, *Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale*, in AA.VV. (a cura di), *Temi e questioni di diritto dell'Unione europea. Scritti offerti*

Vi è poi una prassi istituzionale sempre più orientata a giustapporre sezioni di sicurezza nazionale e sicurezza europea, al punto che sarebbe in atto una "ibridazione" della cooperazione tra Unione e Stati membri in materia di sicurezza, oltre che tra competenze sovranazionali strumenti giuridici interessati [29]. In effetti, l'Unione ha eretto le basi per interventi normativi che, pure in un'ottica di protezione dei propri interessi e dei valori fondanti, si insinuano in maniera più o meno intensa ed estesa in comparti della sicurezza degli Stati membri. Ciò sta avvenendo anche con un certo consenso degli Stati stessi, se non altro perché i rispettivi rappresentanti spesso esprimono voti favorevoli in Consiglio e non risultano azioni di annullamento di atti legislativi per via di ipotetiche violazioni della (presunta) riserva assoluta di competenza per la sicurezza nazionale; per giunta, non mancano occasioni nelle quali gli Stati membri hanno accennato pubblicamente all'esistenza di una sicurezza europea da difendere [30].

È dunque alla luce di queste evoluzioni che va contestualizzato il rapporto tra norme UE in tema di cybersicurezza e competenza statale nel campo della sicurezza nazionale. Si ritiene, infatti, che l'urgenza di una risposta collettiva alle minacce *cyber* stia emergendo quale interesse generale dell'Unione e che, in ossequio ai principi di leale cooperazione e solidarietà, gli Stati membri debbano allineare il più possibile le rispettive azioni di sicurezza nazionale agli obiettivi dell'UE [31].

---

a Caludia Morviducci, Cacucci, Bari, 2019, p. 27 s.; F. CASOLARI, *Leale cooperazione tra Stati membri e Unione europea: studio sulla partecipazione all'Unione al tempo delle crisi*, Editoriale Scientifica, Napoli, 2020, p. 203 ss.

[29] F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited*, in *European Foreign Affairs Review*, 2023, vol. 28, n. 4, p. 339.

[30] Si segnala, ad esempio, la Dichiarazione di Versailles, adottata in occasione della riunione informale dei Capi di Stato o di governo del 10 e 11 marzo 2022. In questo documento gli Stati membri sottolineano l'esigenza di far sì che l'Unione assuma maggiori responsabilità per la "propria" sicurezza, in parte sovrapponendola a quella che gli Stati stessi chiamano "la nostra sicurezza generale". Dal suo canto, la Commissione europea ha affermato che oggi "gli interessi relativi alla sicurezza economica e alla sicurezza nazionale, le vulnerabilità e le risposte degli Stati membri raramente possono essere analizzati o circoscritti indipendentemente da quelli di altri Stati membri o dell'Unione nel suo complesso"; pertanto "(g)li interessi dei singoli Stati membri sono indissolubilmente legati al corretto funzionamento del mercato interno, all'integrità della politica commerciale dell'UE e agli interessi in materia di sicurezza dell'UE nel suo complesso" (COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Strategia europea per la sicurezza economica*, JOIN(2023) 20 final).

[31] S. VILLANI, *The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System*, in *European Journal of Risk Regulation*, 2025, vol. 16, n. 2. p. 495.

2.4. Brevi cenni ai principali fondamenti giuridici dell'azione UE nella dimensione esterna

L'analisi delle competenze di cui l'Unione può disporre per adottare atti vincolanti nel campo della cybersicurezza impone uno sguardo al di là della dimensione interna dell'organizzazione. Infatti, anche l'azione esterna UE sta diventando un interessante terreno di sperimentazione per tentare di addivenire a un complesso normativo più organico sulla cybersicurezza. Ciò specialmente per due ragioni, collegate ad altrettante politiche dell'Unione.

La prima ragione è da rinvenirsi nella competitività di un'Unione che, come accennato in premessa, si è autoimposta di raggiungere obiettivi di ampio respiro, come una sovranità digitale e una autonomia strategica (aperta). Uno dei principali effetti di natura costituzionale di questa transizione è il tentativo di apertura della politica commerciale comune (PCC) agli interessi che l'Unione associa alla cybersicurezza. Infatti, analogamente a quanto visto quando si è discussa l'estensione della superficie d'azione dell'art. 114 TFUE, anche l'art. 207 TFUE, base giuridica (principale) per le iniziative UE di PCC, viene ad oggi utilizzato per disciplinare profili della cybersicurezza. Questo approccio non riguarda esclusivamente taluni atti legislativi con i quali l'Unione cerca di limitare ingerenze esterne di vario tipo [32], ma sta prendendo forma, sebbene ancora limitatamente, anche in diverse categorie di accordi e altri strumenti di natura multilaterale che l'Unione ha concluso di recente con Stati terzi [33].

La seconda ragione va rintracciata negli obiettivi propri dell'azione esterna dell'Unione che, ai sensi dell'art. 21, par. 2, lett. a), TUE, è volta a difendere i propri interessi e proiettare i propri valori nel contesto globale, prestando altresì attenzione alla sua sicurezza, indipendenza ed integrità. Pertanto, anche nel cyberspazio, l'Unione è chiamata a intervenire esercitando la propria competenza nelle nuove declinazioni della politica estera e di sicurezza comune (PESC) i cui profili sono disciplinati nel Titolo V del TUE. Sebbene, infatti, detta politica non contempli espressamente la cybersicurezza tra i propri ambiti di intervento, l'art. 24, par. 1, TUE attribuisce all'Unione la competenza a occuparsi di "tutti i settori della politica estera e tutte le questioni relative alla sicurezza dell'Unione".

---

[32] Cfr. S. POLI-D. GALLO, *Enhancing European Technological Sovereignty: The Foreign Investment Screening Regulation and Beyond*, in K.A. ARMSTRONG-J. SCOTT-A. THIES (eds), *EU External Relations and the Power of Law. Liber Amicorum in Honour of Marise Cremona*, Oxford, Hart Publishing, 2024, p. 215 s.

[33] Ci si riferisce, in particolare, ai partenariati digitali conclusi con Giappone, Repubblica di Corea, Singapore e Canada, e agli accordi sul commercio digitale conclusi con Corea e Singapore. L'impegno a concludere detti strumenti di natura multilaterale è stato promosso nella comunicazione della COMMISSIONE EUROPEA, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM (2021) 118 final, punto 6.

Su tali premesse, l'Unione ha progressivamente inquadrato la cybersicurezza all'interno della PESC, estendendo così la portata materiale di quest'ultima al dominio digitale. Tale evoluzione, pur coerente con la crescente rilevanza delle minacce *cyber* per la sicurezza europea, solleva interrogativi circa l'estensione e i limiti delle competenze dell'Unione in assenza di una base giuridica specificamente dedicata alla disciplina del cyberspazio. Ciononostante, in un'epoca di forti sconvolgimenti geopolitici con evidenti ricadute anche in Europa, la PESC funge più che mai da incubatore per l'elaborazione di strategie e strumenti volti a contrastare quelle minacce perpetrate attraverso mezzi informatici sempre più sofisticati e atte a destabilizzare l'Unione e gli Stati membri in più modi: ad esempio, agendo contro infrastrutture critiche, servizi necessari, funzioni essenziali degli Stati membri, per non parlare della propaganda e delle campagne di disinformazione [34].

Ne consegue che la PESC si configura, oggi, come un laboratorio istituzionale in cui l'Unione sperimenta nuove forme di azione esterna in ambiti tradizionalmente riservati agli Stati membri, estendendo i confini del proprio intervento in materia di sicurezza (digitale) e contribuendo, seppure in via indiretta, al processo di costituzionalizzazione del cyberspazio europeo.

3. Gli strumenti normativi dell'Unione in materia di cybersicurezza: una panoramica

Come emerso fin qui, l'evoluzione delle competenze esercitate dall'Unione in materia di cybersicurezza riflette una progressiva maturazione giuridica, istituzionale e politica rispetto alla sua natura intrinsecamente strategica. Detta evoluzione si traduce, inevitabilmente, nella portata sostanziale dei diversi strumenti giuridici adottati per disciplinare – sotto molteplici profili – l'ambito in oggetto.

La già citata comunicazione del 2020 titolata *La strategia dell'UE in materia di cibersicurezza per il decennio digitale* ha innescato tanto la riforma di alcuni strumenti già esistenti quanto l'adozione di nuovi per garantire che tutti possano "vivere in sicurezza la propria vita digitale" e creare "un'Europa digitale, verde e resiliente" [35]. Un obiettivo, questo, complessivamente ribadito anche nel

[34] In argomento, v. L. LONARDO (ed.), *Addressing Hybrid Threats European Law and Policies*, Cheltenham-Northhampton, Edward Elgar, 2024.

[35] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, cit.

Piano per la cybersicurezza adottato dal Consiglio nel giugno 2025 [36]. Gli sviluppi più recenti mostrano, in effetti, un chiaro orientamento verso la costruzione di un sistema inteso a rafforzare la resilienza collettiva dell'Unione, a promuovere la fiducia nel mercato digitale e a consolidare la capacità europea di reagire in modo unitario alle minacce informatiche che abbiano origine tanto all'interno quanto all'esterno del territorio dell'Unione [37]. Gli strumenti di seguito illustrati – di cui verranno sommariamente evidenziati gli aspetti principali – esprimono una logica che va oltre il mero coordinamento o l'armonizzazione normativa. Pur con alcuni profili da attenzionare quanto al rapporto con le prerogative statali come evidenziato nel paragrafo precedente, essi incarnano il tentativo di tradurre in pratica il paradigma della sovranità digitale europea basata sui valori dell'art. 2 TUE e di integrare la cybersicurezza nel progetto di autonomia strategica sovranazionale.

3.1. La direttiva NIS 2: verso un livello comune elevato di sicurezza delle reti e dei sistemi informativi

Con l'adozione della direttiva (UE) 2022/2555 (c.d. "NIS 2"), in vigore dal 16 gennaio 2023 e applicabile dal 17 ottobre 2024, il legislatore europeo ha inteso superare i limiti emersi nell'attuazione della prima direttiva NIS del 2016. Quest'ultima, pur costituendo, come già detto, il primo tentativo di definire un quadro comune in materia di cybersicurezza, lasciava agli Stati membri un ampio margine di discrezionalità, tipico dello strumento della direttiva, in un contesto caratterizzato da livelli disomogenei per maturità e capacità operative. Tale frammentazione, accentuata dalla scarsa condivisione delle informazioni rilevanti, aveva ostacolato la formazione di un efficace quadro prescrittivo a livello sovranazionale. Pertanto, l'obiettivo della NIS 2 è quello di garantire un livello comune elevato di cybersicurezza attraverso un quadro più omogeneo di obblighi, responsabilità e meccanismi di cooperazione, basandosi sul c.d. "approccio al rischio", coerentemente con la recente legislazione dell'Unione in materia digitale [38].

Tra gli aspetti di maggiore rilievo figura l'ampliamento dell'ambito soggettivo: la direttiva include ora, accanto agli operatori di servizi essenziali, un

---

[36] Raccomandazione del Consiglio del 6 giugno 2025 relativa a un programma dell'UE per la gestione delle crisi informatiche, GU C C/2025/3445, 20 giugno 2025.

[37] Per una ricostruzione del concetto di "resilienza" in materia di cybersicurezza a livello sovranazionale, si veda P.G. CHIARA-R. BRIGHI, *La dimensione della "resilienza" nel diritto UE della cybersicurezza*, in *Ragion Pratica*, 2024, vol. 2, pp. 405-426.

[38] Per approfondimenti, G. DE GREGORIO-P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 2022, vol. 59(2), pp. 473-500.

numero più ampio di soggetti pubblici e privati che operano in settori critici (energia, trasporti, sanità, infrastrutture digitali, pubblica amministrazione centrale e regionale, servizi di comunicazione elettronica, gestione dei rifiuti, produzione e distribuzione alimentare, ecc.) [39]. Il criterio dimensionale ("*size-cap rule*"), secondo cui tutte le entità di medie e grandi dimensioni nei settori interessati rientrano nell'ambito di applicazione della direttiva, costituisce un elemento innovativo, volto ad assicurare coerenza nella designazione dei soggetti obbligati e a limitare la discrezionalità nazionale che aveva caratterizzato la fase di attuazione della prima direttiva NIS [40].

Sotto il profilo sostanziale, la NIS 2 introduce obblighi di gestione del rischio e di notifica degli incidenti più rigorosi, imponendo agli organi di amministrazione un ruolo attivo nella supervisione delle misure di sicurezza. Oltre a richiedere in modo più pregnante agli Stati membri di adottare delle strategie nazionali per la cybersicurezza e designare autorità competenti, punti di contatto unici nonché uno o più gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), essa rafforza il sistema di cooperazione sovranazionale, istituendo reti come la *European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)* e il *Group of Cooperation* [41]. Questi organismi sono concepiti per garantire un coordinamento stabile e strutturato tra le autorità nazionali competenti, nonché per facilitare lo scambio di informazioni, l'assistenza reciproca e la gestione congiunta delle crisi informatiche. Peraltro, nell'ottica di risolvere una delle debolezze strutturali della direttiva precedente, la NIS 2 istituisce da una parte delle procedure per la creazione di accordi volontari di condivisione di informazioni pertinenti alla cybersicurezza [42].

È evidente che, restando una direttiva, la NIS 2 lascia comunque un margine di discrezionalità agli Stati membri in fase di trasposizione ed attuazione. Di conseguenza, l'effettività del quadro delineato dipende in misura determinante dal funzionamento di tali meccanismi di coordinamento e dall'applicazione sostanziale del principio di leale cooperazione di cui all'art. 4, par. 3, TUE, che impone a Stati e istituzioni dell'Unione di agire in uno spirito di fiducia reciproca per garantire – in questo caso specifico – un livello comune elevato di cybersicurezza nel mercato interno. Dal punto di vista sistemico, però, la NIS 2 costituisce un tassello essenziale nella costruzione della strategia digitale dell'Unione. Essa tende a ridurre la frammentazione del mercato interno e a promuovere un livello minimo di resilienza comune, rafforzando al contempo la responsabilità pubblica e privata nella tutela della sicurezza (collettiva) europea.

---

[39] Allegati I (settori ad alta criticità) e II (altri settori critici), Direttiva NIS 2.

[40] Art. 2, parr. 2, 3, 4, Direttiva NIS 2.

[41] Art. 16, Direttiva NIS 2.

[42] Art. 29, Direttiva NIS 2.

3.2. Il *Cybersecurity Act* e il *Cyber Resilience Act*: certificazione e sicurezza dei prodotti digitali

Con il regolamento (UE) 2019/881 (c.d. "*Cybersecurity Act*") [43], l'Unione ha compiuto un passo ulteriore verso la costruzione di un ecosistema digitale sicuro, prevedendo innanzitutto una definizione sovranazionale di "cybersicurezza" che ricomprende "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* [enfasi aggiunta]" [44]. Si delinea, dunque, un'esigenza di sicurezza che non si esaurisce nella protezione delle infrastrutture digitali, ma si estende alla tutela degli individui – che ne sono parte integrante in qualità di "consumatori" – in un'ottica di matrice costituzionale. La cybersicurezza emerge così come condizione abilitante per l'esercizio effettivo dei diritti fondamentali nello spazio digitale, in particolare del diritto alla protezione dei dati personali e alla vita privata, ma anche della libertà di espressione e di informazione [45].

Il *Cybersecurity Act* si articola in due parti, che rispondono a finalità tra loro complementari.

Nella prima parte viene specificato e potenziato il ruolo dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) [46], attribuendole un mandato permanente, con nuovi obiettivi, compiti e aspetti organizzativi [47]. Tramite l'attività dell'ENISA, il regolamento promuove altresì lo sviluppo delle capacità operative e scientifiche dell'Unione in questo settore. A tal fine, sono poste le

---

[43] Per un commento, si veda G.G. FUSTER-L. JASMONTAITE, *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in M. CHRISTEN-B. GORDIJN-M. LOI (eds), *The Ethics of Cybersecurity*, Cham, Springer 2020, pp. 97-115; C. KOHLER, *The EU Cybersecurity Act and European standards: an introduction to the role of European standardization*, in *International Cybersecurity Law Review*, 2020, vol. 1, pp. 7-12.

[44] Art. 2, par. 1, *Cybersecurity Act*.

[45] Per approfondimenti di carattere generale, si veda A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *Quaderni AISDUE*, n. 15, 14 marzo 2023, pp. 321-343; C. AMALFITANO-F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO-S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, Giappichelli, 2023, pp. 1-34; M. DUNN CAVELTY-C. KAVANAGH, *Cybersecurity and human rights*, in B. WAGNER-M.C. KETTEMANN-K. VIETH-DITLMANN-S. MONTGOMERY (eds), *Research Handbook on Human Rights and Digital Technology. Global Politics, Law and International Relations*, Cheltenham, Edward Elgar, 2025, pp. 70-93.

[46] L'Agenzia è stata istituita con il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, GU L 77, 13 marzo 2004.

[47] Art. 1, par. 1, lett. a), *Cybersecurity Act*.

basi per la creazione di una rete europea di centri di competenza in materia di cybersicurezza, il cui coordinamento è affidato al Centro europeo di competenza per la cybersicurezza nell'industria, nella tecnologia e nella ricerca (*European Cybersecurity Competence Centre* – ECCC) [48]. Questo assetto mira a favorire la circolazione delle conoscenze, la sinergia tra ricerca e industria e, in ultima analisi, il rafforzamento dell'autonomia tecnologica e strategica europea rendendola in grado di sviluppare le proprie capacità in materia di cybersicurezza [49].

Nella seconda parte, il *Cybersecurity Act* istituisce un quadro europeo per la certificazione della cybersicurezza. Il sistema di certificazione, strutturato su tre livelli di garanzia (basso, sostanziale, alto), intende fornire agli operatori economici e agli utenti una misura affidabile della sicurezza dei prodotti, servizi e processi ICT [50], in coordinamento con la NIS 2. L'obiettivo ultimo è evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione in materia di cybersicurezza, rafforzando la fiducia dei consumatori [51]. Infatti, "la mancanza di programmi di certificazione riconosciuti in tutta l'Unione che integrino parametri più elevati di resilienza nei prodotti in modo da sostenere la fiducia del mercato a livello dell'UE" è vista dalla Commissione come un ostacolo alla crescita del mercato (interno) della cybersicurezza nell'UE [52].

Con la sua natura di regolamento, direttamente applicabile negli ordinamenti nazionali, il *Cybersecurity Act* pone le basi per un modello di integrazione normativa più incisiva, che trova continuità nel successivo regolamento (UE) 2024/2847 (c.d. *Cyber Resilience Act* o CRA), entrato in vigore il 10 dicembre 2024 e applicabile dall'11 dicembre 2027. Come approfonditamente illustrato in altri capitoli del Volume [53], il CRA segna il passaggio da una logica volontaria a una imposizione normativa di requisiti minimi obbligatori per i

---

[48] Nel dicembre 2020, Bucarest è stata scelta come sede per ospitare il centro, istituito con il regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento, GU L 202, 8 giugno 2021.

[49] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 final, p. 12.

[50] Art. 56, par. 2, *Cybersecurity Act*.

[51] Art. 1, par. 1, lett. b), *Cybersecurity Act*.

[52] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, cit., p. 5.

[53] Per una panoramica generale, si rinvia al capitolo di P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il Cyber Resilience Act*, in questo volume.

prodotti con elementi digitali. Mantenendo un approccio basato sul rischio, il regolamento richiede infatti a fabbricanti, importatori e distributori di garantire la sicurezza lungo l'intero ciclo di vita del prodotto, introducendo obblighi di *due diligence,* tra cui quelli di gestione delle vulnerabilità, di documentazione e informazione, di segnalazione e di cooperazione [54].

Complessivamente, *Cybersecurity Act* e CRA delineano un sistema integrato di sicurezza del mercato digitale europeo, in cui la fiducia e la trasparenza diventano fattori competitivi. Entrambi gli strumenti, prevedendo requisiti tecnici e promuovendo una certificazione europea sulla base di *standard* condivisi, rappresentano strumenti normativi di sovranità digitale, attraverso i quali l'Unione mira a consolidare la propria capacità normativa e tecnologica nel settore della cybersicurezza. Da una parte, il *Cybersecurity Act* attribuisce all'Unione la competenza a definire schemi comuni di certificazione per i prodotti, i servizi e i processi ICT, ponendo le premesse per la creazione di un mercato interno della sicurezza informatica fondato su *standard* armonizzati e condivisi. Dall'altra, il CRA intende definire i requisiti a cui i prodotti digitali devono conformarsi per poter essere commercializzati sul territorio dell'Unione.

In una prospettiva di più ampio respiro, pare evidente che i requisiti di sicurezza assumono necessariamente anche una valenza extraterritoriale: gli schemi adottati a livello dell'Unione tendono a fissare parametri tecnici e procedurali destinati a incidere anche sui soggetti stabiliti al di fuori del territorio dell'UE, qualora intendano immettere prodotti o servizi nel mercato europeo [55]. Tale effetto di proiezione normativa, si allinea sul piano teorico con l'esigenza dell'Unione di affermare i propri valori declinati concretamente in *standard* di sicurezza, contribuendo a definire la prassi internazionale in materia e a ridurre la dipendenza da schemi di certificazione esterni. In tal modo, l'azione dell'Unione non solo rafforza la resilienza interna, ma consolida la sua posizione come (potenziale) attore normativo nel campo della cybersicurezza a livello globale.

3.3. Il *Cyber Solidarity Act*: la dimensione solidaristica della cybersicurezza

Il regolamento (UE) 2025/38 (c.d. "*Cyber Solidarity Act*"), proposto dalla Commissione il 18 aprile 2023 ed entrato in vigore all'inizio del 2025,

---

[54] Si veda, per tutti, l'art. 13, CRA.

[55] E. FAHEY, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford, Oxford University Press, 2022. Sul punto, si rimanda alle riflessioni di V. REMONDINO, *Il Cyber Resilience Act come strumento per la protezione dei valori dell'UE? Tra esigenze di sicurezza dei prodotti e tutela dei diritti fondamentali dei singoli*, in questo volume.

rappresenta l'ultimo tassello del mosaico normativo volto a rafforzare il quadro sovranazionale in materia di cybersicurezza. Esso si innesta nel quadro di cooperazione già delineato dalla direttiva NIS 2 e dagli strumenti operativi esistenti, con l'obiettivo di potenziare la capacità dell'UE di rilevare, prevenire e rispondere a incidenti di cybersicurezza significativi o su vasta scala.

Il regolamento si articola attorno a tre pilastri principali:

i. la creazione di un sistema europeo di allerta per la cybersicurezza, basato su una rete di poli informatici nazionali e transfrontalieri incaricati di favorire la condivisione di informazioni e l'analisi congiunta delle minacce;
ii. l'istituzione di un meccanismo per le emergenze di cybersicurezza, volto a sostenere azioni di preparazione, risposta e assistenza reciproca;
iii. la previsione di un meccanismo europeo di riesame degli incidenti, destinato a trarre insegnamenti strategici dagli attacchi significativi.

Il primo pilastro riflette l'esigenza di sviluppare una *situational awareness* comune attraverso strumenti di cooperazione tecnica. I poli informatici, istituiti su base volontaria ma sostenuti da fondi dell'Unione e dall'ECCC, operano in stretto raccordo con la rete dei CSIRT, *EU-CyCLONe* e le autorità designate ai sensi della direttiva NIS 2 [56].

Il secondo pilastro, il meccanismo per le emergenze, istituisce la *Cybersecurity Reserve* (o "riserva per la cybersicurezza") costituita da un insieme di "fornitori di fiducia" privati incaricati di offrire servizi di risposta su richiesta degli Stati (membri e – sotto certe condizioni – anche terzi) o delle istituzioni dell'Unione [57].

Infine, il meccanismo di riesame degli incidenti consolida un approccio di *learning by doing*: su richiesta della Commissione o di ENISA, in collaborazione con gli Stati interessati, effettua valutazioni *ex post* degli attacchi per migliorare la capacità preventiva e correttiva dell'Unione [58].

Questi meccanismi riflettono un'applicazione funzionale del principio di solidarietà che riveste un ruolo privilegiato nei contesti emergenziali e, specialmente, di fronte a minacce aventi carattere transfrontaliero, come possono rivelarsi quelle legate alla dimensione cibernetica. In effetti, tale principio – ponendosi ad integrazione e supporto del principio di leale cooperazione – rappresenta uno snodo essenziale e obiettivo del regolamento laddove si richiede la condivisione tempestiva di informazioni nonché il dispiegamento immediato di risorse comuni e capacità operative. Il *Cyber Solidarity Act* è pertanto complementare ad altri strumenti e meccanismi che permettono all'UE di reagire a

[56] Artt. 3-9, *Cyber Solidarity Act*.

[57] Artt. 10-20, *Cyber Solidarity Act*.

[58] Art. 21, *Cyber Solidarity Act*.

minacce, incidenti e catastrofi, come il meccanismo europeo di protezione civile, i dispositivi integrati di risposta politica alle crisi (IPCR), la clausola di mutua difesa (art. 42, par. 7, TUE) e la clausola di solidarietà (art. 222 TFUE) [59].

Il *Cyber Solidarity Act*, pur ribadendo che l'attivazione dei meccanismi di assistenza deve avvenire nel rispetto delle prerogative degli Stati in materia di sicurezza nazionale, valorizza così la funzione di coordinamento dell'Unione quale catalizzatore di cooperazione. In effetti, come si è già avuto modo di evidenziare in precedenza, la crescente interdipendenza delle infrastrutture digitali e la dimensione transnazionale delle minacce rendono sempre più labile la linea di demarcazione tra sicurezza nazionale e sicurezza europea. In tal senso, un elemento innovativo del regolamento è rappresentato dall'estensione della riserva europea per la cybersicurezza anche alle istituzioni, agli organi e alle agenzie dell'UE [60]. Queste ultime possono richiedere assistenza in caso di incidenti significativi che minaccino la sicurezza delle infrastrutture o dei processi democratici europei; si pensi, ad esempio, a un attacco volto a interferire con le elezioni del Parlamento europeo o ad accedere a documenti riservati dell'Unione. Tale previsione rappresenta un salto qualitativo non solo teorico ma anche potenzialmente concreto verso una sorta di "europeizzazione" della sicurezza: l'Unione si dota così di strumenti propri di difesa cibernetica, che operano in parallelo e non in sostituzione delle prerogative nazionali, rafforzando così la tutela dell'integrità istituzionale e della sovranità europea.

In definitiva, il *Cyber Solidarity Act* stabilisce un avanzamento nella costruzione di una solidarietà europea in materia di cybersicurezza, trasformando la cooperazione intergovernativa in un meccanismo strutturato e finanziato a livello dell'Unione. Detto regolamento rappresenta così un esperimento di "costituzionalizzazione del cyberspazio", in cui la sicurezza diventa terreno di integrazione e la solidarietà si traduce in un nuovo livello di responsabilità condivisa tra Unione e Stati membri nella difesa dello spazio digitale europeo.

3.4. Strumenti di azione esterna in materia di cybersicurezza: le misure restrittive poste a tutela dell'ordine costituzionale europeo

Come si è già avuto modo di accennare, nel quadro della sua azione ester-

[59] Per approfondimenti sulla portata di dette disposizioni, si veda S. BLOCKMANS, *L'Union fait la Force: Making the Most of the Solidarity Clause (Art 222 TFEU)*, in I. GOVAERE-S. POLI (eds), *EU Management of Global Emergencies. Legal Framework for Combating Threats and Crises*, Leiden, Brill, 2014, pp. 111-135; A. BIONDI-E. DAGILYTÉ-E. KÜÇÜK (eds), *Solidarity in EU Law. Legal principle in the Making*, Cheltenham-Northampton, MA, Edward Elgar 2018; N. NOVÁKY, *The Invocation of the European Union's Mutual Assistance Clause: A Call for Enforced Solidarity*, in *European Foreign Affairs Review*, 2017, pp. 357-375.

[60] Artt. 14-16, *Cyber Solidarity Act*.

na l'Unione europea ha progressivamente costruito un articolato sistema di strumenti volto a contrastare le minacce informatiche di origine esterna e a promuovere un cyberspazio sicuro, aperto e rispettoso dell'integrità dell'ordine costituzionale europeo. In tale prospettiva, è stato progressivamente elaborato il concetto di "cyber diplomazia", espressione di un approccio che combina strumenti di natura diplomatica e giuridica per migliorare il coordinamento internazionale nella gestione delle minacce informatiche e, al contempo, per promuovere un modello di *governance* del cyberspazio ispirato ai valori fondamentali dell'Unione.

Il Quadro per una risposta diplomatica congiunta alle attività informatiche dannose (c.d. "*Cyber Diplomacy Toolbox*"), adottato dal Consiglio nel 2017, costituisce il principale riferimento operativo di tale approccio [61]. Esso delinea un sistema di risposta flessibile e multilivello, volto, da un lato, a rafforzare la cooperazione con Stati terzi e organizzazioni regionali (tra cui la NATO) e, dall'altro, a consentire l'attivazione coordinata dell'intero spettro di strumenti di politica estera dell'Unione – diplomatici, economici e giuridici – in caso di incidenti di cybersicurezza di origine esterna.

In questo contesto, vale la pena approfondire – senza pretesa di esaustività – il regime autonomo di misure restrittive contro gli attacchi informatici, introdotto nel 2019 con la decisione (PESC) 2019/797 e il regolamento (UE) 2019/796 [62]. Detto regime consente all'Unione di imporre sanzioni mirate a persone fisiche o giuridiche, entità o organismi ritenuti responsabili di attacchi informatici o di tentativi di attacco, nonché a coloro che forniscono sostegno finanziario, tecnico o materiale a tali attività o che vi partecipano in qualsiasi forma [63].

Le misure restrittive comprendono, in particolare, il divieto di ingresso nel

---

[61] Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica"), 19 giugno 2017. Per commenti, Y. MIADZVETSKAYA-R.A. WESSEL, *The Externalisation of EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox*, in *European Papers*, 2022, vol. 7, pp. 413-438.

[62] Decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GU L 129I, 17.5.2019 e Regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GU L 129I, 17.5.2019. Per approfondimenti di natura critica, si rinvia a S. POLI-E. SOMMARIO, *The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions*, in *German Law Journal*, 2023, vol. 24, pp. 522-536; F. CASOLARI, *EU Sanctions Policy: A Legal Appraisal in Light of the EU's Strategic Autonomy Doctrine*, in G. ADINOLFI-A. LANG-C. RAGNI (eds), *Sanctions By and Against International Organizations. Common Issues and Current Developments*, Cambridge/Antwerp/Chicago, Intersentia, 2024, pp. 29-57.

[63] Artt. 1 e 7, Regolamento (PESC) 2019/796.

territorio dell'Unione e il congelamento dei fondi e delle risorse economiche appartenenti, posseduti, detenuti o controllati dai soggetti elencati nei rispettivi allegati. Spetta poi agli Stati membri determinare le norme sanzionatorie applicabili in caso di violazione delle misure adottate, garantendo un'applicazione coerente e uniforme a livello dell'Unione.

Gli attacchi informatici rilevanti ai fini dell'attivazione del regime sono quelli che, cumulativamente, possiedono due elementi: producono effetti significativi e sono estranei rispetto al territorio dell'Unione [64]. Pertanto, rientrano in tale categoria gli attacchi provenienti o sferrati dall'esterno, quelli che utilizzano infrastrutture situate fuori dal territorio dell'UE, quelli compiuti da persone o entità stabilite o operanti al di fuori dell'Unione, nonché quelli sostenuti o agevolati da soggetti terzi extra-UE. Il regime contempla, in particolare, gli attacchi diretti contro infrastrutture critiche o servizi essenziali per la società, l'economia o la sicurezza – come i settori dell'energia, dei trasporti, della sanità, dell'acqua potabile, delle infrastrutture digitali e dei mercati finanziari – oltre a quelli che colpiscono funzioni statali fondamentali quali la difesa, i processi elettorali, la sicurezza interna e le missioni diplomatiche. Va evidenziato che gli attacchi informatici, così come le relative minacce, possono essere diretti tanto contro le istituzioni dell'Unione o i suoi Stati membri, quanto nei confronti di Stati terzi o organizzazioni internazionali.

L'individuazione dei soggetti destinatari delle sanzioni avviene *case by case*, prevedendo che il Consiglio svolga una valutazione di natura tanto tecnica quanto politica. Per questo, il regime presenta alcune criticità, tra cui l'elevato grado di discrezionalità degli Stati membri, la difficoltà di provare l'origine esterna degli attacchi e la complessità tecnica di determinare la portata dell'impatto [65]. Elementi, questi, che rischiano invero di indebolire l'efficacia e la coerenza del sistema, esponendolo a tensioni con i principi di certezza del diritto, trasparenza e tutela giurisdizionale sanciti dal diritto primario dell'Unione. Per questo, va ricordato che il regime è soggetto al controllo giurisdizionale della Corte di giustizia dell'Unione europea: le persone ed entità designate possono impugnare le misure ai sensi dell'art. 275 TFUE, assicurando così un livello di tutela che, pur limitato, contribuisce a bilanciare la discrezionalità politica del

---

[64] Art. 1, Decisione (PESC) 2019/797.

[65] Per riflessioni sul punto, Y. MIADZVETSKAYA, *Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP)*, in A. VEDDER-J. SCHROERS-C. DUCUING-P. VALCKE (eds), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Cambridge/Antwerp/Chicago, Intersentia 2019, pp. 277-298; I. BOGDANOVA-M. VASQUEZ CALLO-MULLER, *Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value*, in *Vanderbilt Law Review*, 2023, vol. 54, pp. 911-954.

Consiglio con le esigenze di legalità e di rispetto dei diritti fondamentali [66].

Sulla base della decisione (PESC) 2019/797, dal 2020 il Consiglio ha adottato varie decisioni di misure restrittive nei confronti di individui e gruppi collegati a episodi di cyber attacchi di rilievo internazionale. Tra queste, merita innanzitutto ricordare quelle relative ai noti casi *WannaCry* e *NotPetya*, che avevano colpito reti informatiche globali mediante ransomware, causando gravi danni economici [67]. Successivamente, nell'ottobre 2020, sono stati inseriti nella lista altri soggetti per il tentato attacco informatico contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) all'Aia e per l'attacco ai sistemi informatici del Bundestag tedesco nel 2015, attribuiti ad agenti dell'intelligence russa [68].

In seguito a revisioni periodiche, tali misure restrittive sono state rinnovate annualmente e ulteriormente estese. Il 24 giugno 2024, il Consiglio ha adottato una nuova serie di sanzioni nei confronti di sei persone fisiche, con il sostegno anche di diversi Paesi terzi (tra cui Macedonia del Nord, Montenegro, Albania, Ucraina, Moldavia, Bosnia-Erzegovina e i Paesi EFTA Islanda e Norvegia). Il 27 gennaio 2025, ulteriori misure sono state adottate contro tre ufficiali dell'intelligence militare russa (unità GRU 29155), ritenuti responsabili di una serie di attacchi informatici contro la Repubblica di Estonia nel 2020, che avevano comportato accessi non autorizzati a dati sensibili detenuti da vari ministeri governativi [69].

Questa ricca casistica dimostra come l'Unione tenda a utilizzare le misure restrittive non solo come strumento reattivo, ma anche come mezzo di dissuasione normativa e diplomatica, volto a riaffermare la legittimità del proprio ordine giuridico nel cyberspazio. In questo senso, le misure restrittive non si limitano a tutelare la sicurezza esterna, ma concorrono a difendere, per certi versi, la sicurezza costituzionale europea, intesa come insieme di valori comuni e co-

---

[66] C. ECKES, *EU restrictive measures against natural and legal persons: From counterterrorist to third country sanctions*, in *Common Market Law Review*, 2014, vol. 51, pp. 869-905; S. POLI, *Judicial Challenges to EU Restrictive Measures by Individual State Organs, 'Emanations of Non-EU Member States' and Third Countries: The Limits to the Council's Discretion*, in G. ADINOLFI-A. LANG-C. RAGNI (eds), *Sanctions By and Against International Organizations: Common Issues and Current Developments*, cit., pp. 203-224.

[67] Regolamento di esecuzione (UE) 2020/1125 del Consiglio del 30 luglio 2020 che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GU L 246, 30.7.2020.

[68] Regolamento di esecuzione (UE) 2020/1536 del Consiglio del 22 ottobre 2020 che attua il regolamento (EU) 2019/796 concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GU L 351I, 22 ottobre 2020.

[69] Regolamento di esecuzione (UE) 2025/173 del 27 gennaio 2025 che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GU L 2025/173, 27 gennaio 2025.

me nucleo identitario sovranazionale. Al tempo stesso, l'efficacia di queste misure dipende, e dipenderà in prospettiva, dalla capacità sovranazionale di garantire un equilibrio tra detta tutela e il rispetto dei principi di legalità, coerenza e trasparenza che caratterizzano l'ordinamento stesso dell'Unione.

4. Conclusioni

L'analisi svolta nei paragrafi che precedono delinea una progressiva incidenza trasversale delle tematiche connesse alla cybersicurezza rispetto al *law making* dell'Unione europea. Ancorché siano chiaramente individuabili degli ambiti dell'azione UE specialmente interessati da tali tematiche – ne è un chiaro esempio il mercato interno e, più precisamente, la clausola generale dedicata al corretto funzionamento di quest'ultimo – l'ampiezza dello spettro di intervento dell'Unione è innegabile, tanto sul piano interno quanto su quello esterno. Ciò appare in linea con il fatto che le iniziative discusse in questo contributo si collocano all'interno della dottrina dell'autonomia strategica, la cui portata ha ormai una valenza sistemica. Quest'ultima precisazione consente di evidenziare anche un ulteriore elemento di sviluppo della disciplina sovranazionale sulla cybersicurezza, vale a dire la sua tensione valoriale, che ne fa strumento di tutela degli elementi identitari dell'ordinamento UE. Ciò contribuisce a spiegare anche il fatto che tale disciplina stia contribuendo a ridefinire, assieme ad altre misure adottate dall'Unione nel contesto della sua autonomia strategica [70], un nuovo paradigma securitario sovranazionale, che non si mette in contrapposizione ma semmai integra quello che informa le iniziative assunte dagli Stati membri per la tutela della sicurezza nazionale, favorendo così anche un'integrazione flessibile tra prerogative statali e capacità di intervento dell'Unione.

[70] F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine*, cit.

Capitolo 3

Il quadro della governance della cybersicurezza a livello nazionale

Tommaso F. Giupponi [*]

Abstract: Il contributo ricostruisce, in chiave problematica, la governance della cybersicurezza a livello nazionale, frutto di una recente implementazione legislativa (anche su impulso europeo) culminata con l'istituzione dell'Agenzia per la cybersicurezza nazionale. Tale Agenzia, con funzioni di supporto tecnico e operativo rispetto alle competenze in materia della Presidenza del Consiglio dei ministri, rappresenta uno snodo centrale nel governo multilivello della cybersicurezza. Anche se collocata formalmente all'esterno del perimetro del Sistema di informazione per la sicurezza della Repubblica, molti sono gli snodi e i punti di contatto tra i due comparti, circostanza che pone la necessità di un più efficace coordinamento in materia di cybersicurezza sia all'interno del Governo, sia in relazione agli strumenti di controllo parlamentare esperibili.

Keywords: Cybersicurezza – Sicurezza nazionale – Presidenza del Consiglio dei Ministri – Agenzia per la cybersicurezza nazionale – Controllo parlamentare

1. La cybersicurezza tra ordine pubblico, difesa e sicurezza nazionale

L'evoluzione tecnologica, come noto, ha condizionato in maniera assai significativa le più recenti trasformazioni delle società contemporanee. Tale processo,

[*] Professore Ordinario di Diritto Costituzionale presso il Dipartimento di Scienze Giuridiche dell'Università di Bologna, tommaso.giupponi@unibo.it.

tra le altre cose, ha imposto anche una rilettura di alcune delle categorie giuridiche più consolidate, al fine di adeguarle alla continua (e sempre più rapida) innovazione, giungendo a ridefinire il ruolo stesso degli Stati come comunità politiche organizzate, non solo, sul piano interno, quali veri e propri Stati digitali [1], ma anche sul piano internazionale. Gli strumenti messi a disposizione dall'*Information and Communication Technology* (ICT), alla luce delle loro immense potenzialità, hanno da subito fatto emergere non solo nuovi orizzonti di sviluppo della persona umana e dei suoi diritti fondamentali, ma hanno parallelamente posto un enorme problema di tutela e regolazione rispetto ai rischi connessi ad un loro utilizzo massiccio ed incontrollato.

Alle tradizionali minacce sperimentate nell'arena "materiale" di espressione della sovranità degli Stati, cui tradizionalmente gli ordinamenti hanno risposto attraverso la predisposizione di specifici strumenti ed apparati amministrativi (si pensi, solo per fare un esempio, alla difesa e all'ordine pubblico), si aggiungono ora nuove vulnerabilità dovute all'utilizzo sempre più diffuso dell'ICT nell'ambito delle nuove arene "virtuali", fortemente interconnesse tra loro, le quali rappresentano ormai il terreno privilegiato di azione di singoli individui, operatori economici e pubbliche autorità [2], in un contesto dove i tradizionali confini tra sicurezza interna ed esterna sembrano divenire, a tratti, sempre più sfumati [3].

Anche i pubblici poteri, infatti, utilizzano ormai diffusamente tali strumenti nell'esercizio delle loro funzioni istituzionali, mentre la maggior parte dei servizi essenziali è oggi garantita, organizzata ed erogata grazie alla rete ed alle tecnologie informatiche. Rispetto alle tradizionali infrastrutture "materiali", tuttavia, le infrastrutture "virtuali" evidenziano differenti problemi di tutela rispetto alle potenziali minacce, che richiedono la costruzione di un adeguato impianto normativo, ad alto contenuto tecnico. Proprio per questo, il problema della sicurezza delle reti e degli strumenti di comunicazione è divenuto oggi un problema centrale [4].

---

[1] Sul punto, da ultimo, cfr. L. TORCHIA, *Lo Stato digitale. Una introduzione*, Il Mulino, Bologna, 2025.

[2] R. BALDONI, *Sovranità digitale. Cos'è e quali sono le principali minacce al cyberspazio nazionale*, Il Mulino, Bologna, 2025.

[3] Sul punto, per tutti, G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 2019, n. 4, p. 65 ss.

[4] Secondo il *Rapporto CLUSIT* del 2025, il numero di incidenti informatici rilevati in Italia nel 2024 è aumentato del 15,2% rispetto al 2023, con una tendenza che è comunque in significativo aumento da anni anche a livello globale (www.clusit.it). Sul punto, vedi anche l'ultima *Relazione sull'attività svolta dall'Agenzia per la cybersicurezza nazionale* (presentata al Parlamento il 2 maggio 2025), in base alla quale sono stati rilevati, nel corso del 2024, ben 1.979 eventi *cyber*, con un aumento del 40% rispetto al 2023.

Non è un caso, allora, che sia stato sottolineato come la cybersicurezza [5] assuma oggi tutte le caratteristiche di una vera e propria funzione pubblica, del tutto peculiare, e che rappresenti un possibile nuovo "volto" del potere negli Stati costituzionali liberaldemocratici [6].

È del tutto evidente, infatti, che tale evoluzione ha ridisegnato anche il piano delle relazioni internazionali; nell'attuale scenario politico globale, infatti, gli Stati si fronteggiano non solo nell'ambito dei più tradizionali "domini" consolidati (terrestre, marino, aereo e spaziale), ma anche nel nuovo dominio *cyber*, vero e proprio spazio virtuale interconnesso, dove sempre di più essi agiscono anche nella gestione e risoluzione dei conflitti e delle controversie internazionali, di fronte a minacce di natura sempre più ibrida (si pensi, solo per fare qualche esempio, alla *cyber warfare* e alla *cyber intelligence*) [7].

In questo contesto, non stupisce allora che la *cyber security* (o cybersicurezza) evidenzi più di un collegamento con la tutela della sicurezza nazionale e con gli apparati tradizionalmente posti a sua tutela dagli ordinamenti nazionali. Tuttavia, proprio per la sua trasversalità, il dominio *cyber* richiede parallelamente il coinvolgimento di altri apparati dello Stato, quali l'amministrazione di pubblica sicurezza e quella della difesa, oltre che un significativo apporto degli operatori economici privati.

D'altronde, come noto, lo stesso concetto di sicurezza nazionale ha subito negli ultimi decenni un'evoluzione che ne ha ridefinito natura e confini, anche alla luce della necessità di un suo adeguamento rispetto alle nuove minacce emergenti sullo scenario globale, come il terrorismo internazionale e la stessa criminalità informatica [8]. In questo senso, allora, non è un caso che l'attuale

---

[5] Per un inquadramento del tema, cfr. G. D'ANGELO-G. GIACOMELLO, *Cybersicurezza. Che cos'è e come funzione*, Il Mulino, Bologna, 2023; nonché, con specifico riferimento agli aspetti informatico-giuridici, R. BRIGHI, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica*, in questo volume.

[6] In questo senso, da ultimo, R. URSI, *La sicurezza cibernetica come funzione pubblica*, in Ursi, R. (a cura di), *op. cit.*, p. 7 ss.; E. LONGO, *Il diritto costituzionale e le cybersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna parlamentare*, 2024, n. 2, p. 313 ss. Sul punto, con uno sguardo alle dinamiche europee, vedi anche R. BRIGHI-P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 2021, n. 21, p. 18 ss.

[7] Negli ultimi anni tale tendenza si è manifestata non solo in relazione all'emergenza terroristica internazionale ma, più di recente, anche in occasione di veri e propri conflitti armati, come quello russo-ucraino, e attraverso campagne di disinformazione e di diffusione in rete di *fake news*, volte ad influenzare l'opinione pubblica. Sul punto, da ultimo, vedi la *Relazione annuale sulla politica dell'informazione per la sicurezza* del 2024 (XIX Legislatura, Doc. XXXIII, n. 3), in particolare p. 21 ss., www.sicurezzanazionale.gov.it; www.parlamento.it.

[8] Sul punto, sia consentito un rinvio a T.F. GIUPPONI, *Sicurezza e potere*, in *Enciclopedia del diritto*, *I Tematici*, *Potere e Costituzione*, V, Giuffrè, Milano, 2023, p. 1146 ss.

disciplina in materia di servizi di informazione e segreto di Stato individui, tra le finalità principali di tale particolare apparato normativo, la «integrità della Repubblica, anche in relazione ad accordi internazionali», la «difesa delle istituzioni poste dalla Costituzione a suo fondamento», la «indipendenza […] rispetto agli altri Stati», la «preparazione» e la «difesa militare» [9]. Quanto alle attività dei servizi di *intelligence*, invece, alle due Agenzie viene affidato il compito di acquisire ed analizzare le informazioni volte a proteggere la Repubblica da minacce esterne ed interne (anche rispetto ad attività eversive o terroristiche), al fine di garantire «la protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia» [10]. Infine, si prevede che ai servizi di informazione sia affidata in via esclusiva anche l'attività di controspionaggio, finalizzata a contrastare le attività informative «volte a danneggiare gli interessi nazionali» [11].

Oggi, infatti, l'indipendenza e la sovranità di uno Stato possono essere messe in discussione non solo sul piano dell'aggressione armata o dell'attacco terroristico, ma anche sul piano economico, finanziario, industriale o tecnologico [12]: il riferimento obbligato va, ad esempio, alla stabilità del sistema economico generale, alla sicurezza informatica delle strutture strategiche nazionali, fino ai variegati interessi scientifici e tecnologici convolti dalla c.d. sicurezza sanitaria ed alla accessibilità delle fonti di approvvigionamento energetico, resi evidenti dalla pandemia da Covid-19 e dal più recente conflitto tra Russia e Ucraina. Sullo sfondo, emerge anche la disciplina dei "poteri speciali" del Governo nei settori strategici per la tutela degli interessi nazionali quali la difesa, la sicurezza nazionale, l'energia i trasporti e le comunicazioni (c.d. *golden power*), che ha subito un processo di progressiva implementazione ed estensione, da ultimo proprio in relazione all'evoluzione dei servizi ICT e ai connessi profili di sicurezza cibernetica [13].

---

[9] Così, in particolare, l'art. 39, comma 1, della l. n. 124/2007.

[10] In questo senso, espressamente, gli artt. 6, comma 2, e 7, comma 2, della l. n. 124/2007.

[11] Cfr. gli artt. artt. 6, comma 3, e 7, comma 3, della l. n. 124/2007.

[12] Il dato appare evidente anche dalla lettura della *Relazione sulla politica dell'informazione per la sicurezza* che il Presidente del Consiglio deve presentare al Parlamento entro la fine di febbraio di ogni anno (art. 38 della l. n. 124/2007). Negli ultimi anni, infatti, è emersa progressivamente sempre una maggiore attenzione ai profili di sicurezza economico-finanziaria, energetica ed ambientale, oltre che in materia di *cybersecurity*, anche alla luce della natura sempre più ibrida delle minacce alla sicurezza nazionale. Da ultimo, vedi la già citata *Relazione* annuale, presentata lo scorso 28 febbraio 2025.

[13] Sulla base di quanto previsto dal d.l. n. 21/2012, più volte modificato. Su tali aspetti, si vedano, tra gli altri, B. CAROTTI, *Sicurezza cibernetica e Stato-nazione*, in *Giornale di diritto amministrativo*, 2020, n. 5, p. 629 ss.; G. DELLA CANANEA-L. FIORENTINO (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, Editoriale scientifica, 2020; C. GENGARO,

Tale lettura sembra ora trovare una qualche conferma anche nel dettato normativo. Istituendo l'Autorità per la cybersicurezza nazionale (ACN), infatti, il legislatore ha colto l'occasione per definire la *cyber security* 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»; tuttavia, viene espressamente specificato che rimangono ferme le attribuzioni del Sistema di informazione per la sicurezza della Repubblica e gli obblighi derivanti dai trattati internazionali [14].

Dunque, come vedremo, la cybersicurezza evoca un ambito di intervento piuttosto ampio, multilivello e trasversale, all'interno del quale sono innegabili i collegamenti con il sistema di informazione per la sicurezza, ma che non può essere fatto coincidere, *sic et simpliciter*, con l'area operativa dell'*intelligence*, non fosse altro perché il processo di trasformazione digitale dell'amministrazione pubblica attualmente in corso riguarda trasversalmente tutti i settori, e chiama inevitabilmente in causa anche l'attività degli operatori economici e delle imprese private coinvolte in tale processo [15].

Tuttavia, è fuori discussione che (almeno alle origini) la normativa italiana in materia di *cyber security* sia nata all'interno del Sistema di informazione per la sicurezza della Repubblica, disciplinato, come noto, dalla l. n. 124/2007. Infatti, alla luce delle modifiche introdotte dalla l. n. 133/2012, tra i compiti affidati al Presidente del Consiglio dei ministri, quale Autorità nazionale per la sicurezza della Repubblica, troviamo oggi anche quello di impartire al Dipartimento delle informazioni per la sicurezza (DIS) e alle agenzie di *intelligence* «direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali» [16].

Stato e mercato. Dalla golden share al golden power, Napoli, Editoriale scientifica, 2023. Sul punto, vedi anche quanto previsto dal Regolamento (UE) n. 2019/452 sul controllo degli investimenti esteri diretti all'interno dell'UE, sul quale cfr. G. NAPOLITANO (a cura di), *Foreign Direct Investment Screening. Il controllo sugli investimenti esteri diretti*, Bologna, Il Mulino, 2019.

[14] Vedi quanto stabilito dall'art. 1, comma 1, lett. a), del d.l. n. 82/2021.

[15] Sul punto, tra gli altri, si veda L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informativo*, in *Federalismi.it*, 2022, n. 25, p. 65 ss.

[16] In questo senso l'art. 1, comma 3-*bis*, della l. n. 124/2007, introdotto dalla l. n. 133/2012. A sua volta, il DIS (sulla base di tali direttive) «coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali»; cfr. l'art. 4, comma 3, lett. d-*bis*) della l. n. 124/2007, come modificata dalla già citata l. n. 133/2012. Sulla base di tali previsioni, sono stati adottati i primi provvedimenti in materia di cybersicurezza (cfr.

Tuttavia, la complessità (non solo tecnica) della materia e la necessità di un maggiore coordinamento tra le diverse istituzioni coinvolte, oltre che il particolare rilievo delle imprese private operanti nel settore, hanno fatto emergere molto presto l'impossibilità di una collocazione esclusiva della *cyber security* all'interno del comparto *intelligence*. Questo, a ben vedere, non tanto perché l'attività informativa a tutela della sicurezza nazionale non debba, oggi più che mai, confrontarsi anche con le potenzialità (e le minacce) della rete e delle tecnologie informatiche di comunicazione, quanto perché la progressiva evoluzione tecnologica dell'amministrazione, dei servizi pubblici, delle attività economiche e delle più generali relazioni sociali rende necessario garantire trasversalmente la sicurezza *delle* reti e degli stessi utenti *nelle* reti.

Questa consapevolezza, come vedremo, ha portato l'ordinamento ad un progressivo cambio di passo che, a partire dalle indicazioni provenienti dall'UE, ha recentemente rivisto la complessiva architettura istituzionale della cybersicurezza, attraverso un percorso che, tuttavia, appare ancora in atto e non privo di ambiguità ed incertezze.

2. L'evoluzione della normativa di settore e la sua progressiva stratificazione (e complicazione)

Nella consapevolezza dell'insufficienza di ogni tentativo di regolazione a livello nazionale [17], l'attenzione dell'UE in materia è andata via via crescendo nel corso degli anni, anche al fine di garantire un mercato unico delle tecnologie digitali, assicurando l'affidabilità degli strumenti ITC e *standard* uniformi di protezione degli utenti. Infatti, a partire dall'adozione di una vera e propria strategia europea in materia di *cyber security*, sono stati approvati negli ultimi anni diversi atti normativi particolarmente significativi, volti non solo ad accompagnare la transizione digitale e l'innovazione tecnologica attraverso la garanzia di strumenti affidabili, ma anche a rafforzare la capacità dell'UE e degli Stati membri di resistere a possibili attacchi informatici [18].

---

il d.p.c.m. 24 gennaio 2013 e il successivo d.p.c.m. 17 febbraio 2017, recanti indirizzi per la protezione cibernetica e la sicurezza informatica nazionale), i quali prevedevano una complessa architettura istituzionale, incentrata sulla Presidenza del Consiglio dei ministri, sul DIS, sul Comitato interministeriale per la sicurezza della Repubblica (CISR) nonché, per i profili più squisitamente tecnico-operativi, sul Nucleo per la sicurezza cibernetica (NSC).

[17] Tra le risposte a livello internazionale, si segnala in particolare la Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest nel 2001, entrata in vigore nel 2004 e attualmente ratificata da 69 paesi (per l'Italia, cfr. la l. n. 48/2008).

[18] Sul punto, tra gli altri, si veda E. LONGO, *La disciplina della cybersicurezza nell'Unione*

Due, sostanzialmente, le direttrici seguite: 1) armonizzare gli *standard* di sicurezza previsti dagli ordinamenti nazionali in materia di prevenzione delle (e risposta alle) minacce informatiche in alcuni settori strategici considerati particolarmente rilevanti; 2) rafforzare gli strumenti di cooperazione, prevedendo parallelamente un sistema europeo di certificazione in materia di cybersicurezza, in modo da creare un mercato unico dei relativi servizi.

Sul primo punto, in particolare, è intervenuta dapprima la Direttiva (UE) n. 2016/1148 (*Network and Information Security*, c.d. NIS), attuata tramite il d.lgs. n. 65/2018, recentemente sostituita dalla Direttiva (UE) n. 2022/2555, c.d. NIS 2, attuata dal d.lgs. n. 138/2024. Sul secondo, invece, assumono particolare rilevanza il Regolamento (UE) n. 2019/881 (c.d. *Cybesecurity Act*) nonché, da ultimo, il Regolamento (UE) n. 2024/2847 (c.d. *Cyber Resilience Act*) e il Regolamento (UE) n. 2025/38 (c.d. *Cyber Solidarity Act*). Comune a tutti i più recenti interventi dell'UE in materia, in ogni caso, è il tentativo di un superamento del tradizionale approccio settoriale che aveva contraddistinto i precedenti interventi in materia, attraverso una visione trasversale e multisettoriale alla cybersicurezza [19].

Con le Direttive NIS e NIS 2, in particolare, al fine di introdurre una disciplina minima comune in materia di sicurezza delle reti e dei servizi informativi, sono stati previsti tutta una serie di obblighi in capo agli Stati e ai soggetti operanti nell'ambito dei settori individuati come essenziali e strategici [20].

Quanto agli Stati, è previsto che essi debbano adottare una strategia nazionale in materia di cybersicurezza «per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale», all'interno della quale, tra l'altro, indicare gli obiettivi e le priorità da seguire, il quadro di *governance* previsto, un sistema di valutazione dei rischi, le misure di preparazione, risposta e recupero rispetto

---

europea e in Italia, in S. CALZOLAIO-A. IANNUZZI-E. LONGO-M. OROFINO (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 203 ss.; per una ricostruzione dell'evoluzione normativa europea in materia di cybersicurezza, vedi anche F. CASOLARI-F. FERRI-S. VILLANI, *La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea*,in questo volume.

[19] Vedi, tuttavia, ora il Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act*), il quale prevede prescrizioni specifiche in materia di cybersicurezza per il settore finanziario (sul punto, da ultimo, vedi anche il d.lgs. n. 23/2025).

[20] Con particolare riferimento ai settori dell'energia, dei trasporti, bancario e dei servizi finanziari, di fornitura e distribuzione di acqua, delle infrastrutture digitali (cf. l'Allegato II del d.lgs. n. 65/2018). La Direttiva NIS 2, da ultimo, ha esteso il suo campo di applicazione anche ad altri significativi settori, quali quello sanitario, l'ingegneria aerospaziale, la gestione dei rifiuti, la produzione e distribuzione alimentare, il settore chimico, i servizi postali, le organizzazioni di ricerca, ma anche buona parte della pubblica amministrazione (cfr. gli Allegati I, II, III e IV del d.lgs. n. 138/2024).

alle minacce informatiche, oltre che specifici piani di formazione, sensibilizzazione e ricerca in materia di sicurezza delle reti e dei sistemi informativi [21]. Sempre in capo agli Stati, poi, è previsto l'obbligo di individuare una o più Autorità nazionali in materia di sicurezza informatica, di istituire uno specifico gruppo di intervento per la sicurezza in caso di incidente informatico (*Computer Security Incident Response Team*, c.d. CSIRT), oltre che di prevedere un punto di contatto unico nazionale per garantire un'efficace cooperazione tra l'UE e gli Stati membri [22].

In relazione ai soggetti operanti nell'ambito dei già citati settori strategici, vengono individuati specifici obblighi per i soggetti definiti «essenziali» e per quelli definiti «importanti», con una gradazione che tiene conto del livello di criticità dello specifico settore e della sua interconnessione con altri settori o servizi considerati strategici [23].

Tali soggetti, in particolare, devono adottare misure organizzative e tecniche adeguate e proporzionate per evitare, fronteggiare e gestire eventuali attacchi (o incidenti) informatici diretti alle proprie infrastrutture digitali, notificando al CSIRT Italia gli eventuali episodi che abbiano un impatto rilevante sulla continuità dei servizi forniti [24]. In caso di inadempimento, sono previste specifiche sanzioni amministrative pecuniarie [25].

Quanto al secondo punto, invece, il *Cybersecurity Act* è intervenuto in una duplice direzione, rafforzando il ruolo dell'*European Network and Information Security Agency* (ENISA) [26], e introducendo un quadro comune europeo per la

---

[21] In questo senso, da ultimo, vedi l'art. 9 del d.lgs. n. 138/2024.

[22] Cfr. ora gli artt. 10 e 15 del d.lgs. n. 138/2024, che individuano l'Agenzia per la cybersicurezza nazionale (ACN) quale autorità nazionale e punto di contatto unico, disciplinando al contempo organizzazione e funzionamento del CSIRT Italia.

[23] Tra i primi rientrano, ad esempio, gli operatori del settore energetico, sanitario, spaziale, bancario, dei trasporti, delle infrastrutture digitali e delle acque, oltre che le pubbliche amministrazioni centrali; tra i secondi, invece, sono ricompresi (tra gli altri) i servizi postali, la gestione dei rifiuti, il settore chimico, quello agroalimentare e le organizzazioni di ricerca, cui si aggiungono anche le pubbliche amministrazioni territoriali specificamente individuate (cfr. l'art. 6 del d.lgs. n. 138/2024).

[24] Sul punto, in particolare, si vedano gli artt. 24 e 25 del d.lgs. n. 138/2024. In particolare, è previsto che senza ingiustificato ritardo, e comunque entro 24 ore, debba essere inviata al CSIRT Italia una pre-notifica dell'incidente informatico, seguita da una notifica più dettagliata entro 72 ore, contenente una prima valutazione dell'incidente stesso.

[25] Cfr. l'art. 38 del d.lgs. n. 138/2024.

[26] Istituita (pur provvisoriamente e con limitate funzioni consultive) dal Regolamento (CE) n. 2004/460 e successivamente riformata dal Regolamento (UE) n. 2013/526, oggi l'ENISA svolge un ruolo fondamentale, dovendo supportare gli Stati nell'elaborazione ed attuazione delle politiche di cybersicurezza.

certificazione della sicurezza di prodotti e servizi ICT, mentre il *Cyber Resilience Act* ha introdotto regole volte ad aumentare la sicurezza e resilienza informatica dei prodotti con elementi digitali. Da ultimo, il *Cyber Solidarity Act* ha implementato gli strumenti di cooperazione operativa in relazione agli incidenti informatici aventi un impatto significativo e su larga scala.

In questo senso, appare particolarmente significativa la previsione di una vera e propria rete composta dai diversi gruppi di intervento nazionali per la sicurezza in caso di incidente (c.d. CSIRTs *Network*), cui partecipa anche il gruppo di intervento della stessa UE (c.d. CERT-UE), e il cui Segretariato è incardinato presso l'ENISA [27]. Parallelamente, sempre presso l'ENISA è stato istituito il Segretariato dell'*EU Cyber Crisis Liaison Organization Network* (c.d. EU-CyCLONE), avente lo scopo di garantire una più stretta collaborazione, un costante scambio informativo e un'azione coordinata tra le autorità competenti a gestire le crisi informatiche a livello nazionale, in caso di incidenti su larga scala [28].

A sua volta, il legislatore nazionale è successivamente intervenuto più volte, dapprima attraverso l'istituzione del Perimetro di sicurezza nazionale cibernetica (PSNC), ad opera del d.l. n. 105/2019 [29], nonché, da ultimo, con l'approvazione della l. n. 90/2024, contenente una serie di misure eterogenee miranti a rafforzare la cybersicurezza nazionale [30]. Tali ripetuti interventi, unitamente alla necessità di un costante adeguamento ai provvedimenti europei già citati, hanno finito per costruire un quadro normativo particolarmente complesso ed articolato, a tratti di difficile ricostruzione e non privo di contraddizioni.

---

[27] Come già previsto dall'art. 12, comma 2, della Direttiva NIS, confermato dall'art. 7, comma 3, del *Cybersecurity Act*, e attualmente ribadito anche dall'art. 15 della Direttiva NIS 2. Sul punto, vedi ora anche quanto previsto dall'art. 3 del *Cyber Solidarity Act*, nell'istituire il sistema europeo di allerta per la cybersicurezza.

[28] In base a quanto stabilito dall'art. 16 della Direttiva NIS 2. Secondo quanto ora previsto dall'art. 13 del d.lgs. n. 138/2024, l'ACN e il Ministero della difesa "sono individuati quali Autorità nazionali di gestione delle crisi informatiche", rispettivamente, per la parte relativa alla resilienza nazionale e per la parte relativa alla difesa dello Stato, riconoscendo però una funzione di coordinamento in capo alla stessa ACN.

[29] Su tale intervento normativo, tra gli altri, si vedano S. POLETTI, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro nazionale di sicurezza cibernetica*, in *MediaLaws*, 2023, n. 2, p. 398 ss.; L. CALANDRIELLO, *Il perimetro di sicurezza nazionale cibernetica*, in R. URSI (a cura di), *op. cit.*, p. 139 ss.

[30] Rafforzando il livello di sicurezza informatica, con particolare riferimento alle pubbliche amministrazioni, intervenendo sulla governance della cybersicurezza, potenziando il coordinamento tra i vari soggetti istituzionali coinvolti e affinando, altresì gli strumenti di tutela penale in materia. Su tale provvedimento legislativo, da ultimo, si vedano le osservazioni critiche di L. PREVITI, *La nuova legge sulla cybersicurezza, un passo avanti e due indietro*, in *Giornale di diritto amministrativo*, 2025, n. 1, p. 60 ss.

La finalità dell'istituzione del PSNC, esplicitata fin dalle prime righe del d.l. n. 105/2019, è stata quella di «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» [31].

Il provvedimento in questione ha cercato di dare una risposta unitaria e coordinata alle minacce *cyber* in grado di compromettere la sicurezza nazionale in relazione a settori considerati strategici. Tuttavia, l'architettura istituzionale delineata, oltre che la concreta attuazione delle misure previste dal PSNC, sono apparse subito molto complesse, essendo coinvolte diverse amministrazioni dello Stato, oltre che enti e operatori pubblici e privati, ed essendo richiesti diversi provvedimenti di attuazione del quadro legislativo delineato [32]. In ogni caso, centrale (ancora una volta) è il ruolo della Presidenza del Consiglio dei ministri e del Sistema di informazione per la sicurezza della Repubblica, pur essendo previsto (almeno originariamente) un coinvolgimento importante anche del Ministero dello sviluppo economico, con particolare riferimento alla valutazione e certificazione dei sistemi e servizi ICT [33].

Particolarmente delicata, come può facilmente intuirsi, è l'individuazione delle categorie di soggetti ricompresi nel PSNC, la quale viene demandata (quanto ai criteri generali) ad un apposito d.p.c.m., mentre per l'indicazione puntuale di coloro che rientrano nel perimetro è prevista l'adozione di uno specifico provvedimento amministrativo segretato, sempre da parte del Presidente del Consiglio dei ministri [34]. In base al d.p.c.m. n. 131/2020, «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

[31] Così, espressamente, l'art. 1 del d.l. n. 105/2019.

[32] Cfr., in questo senso, il d.p.c.m. n. 131/2020, il d.p.r. n. 54/2021, il d.p.c.m. n. 81/2021, il d.p.c.m. 15 luglio 2021 nonché, da ultimo, il d.p.c.m. n. 92/2022.

[33] Di competenza del Centro di valutazione e certificazione nazionale (CVCN), previsto dall'art. 1, comma 6, del d.l. n. 105/2019.

[34] Si veda, in questo senso, l'art. 1, comma 2-*bis*, del d.l. n. 105/2019, in base al quale l'elencazione dei soggetti inclusi nel PSNC «è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri […] per il quale è escluso il diritto di accesso» e che «non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco» (vedi, sul punto, anche l'art. 5 del d.p.c.m. n. 131/2020).

relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti»; mentre «presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato […] laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale» [35].

A tali soggetti la normativa richiede non solo l'adozione di adeguate misure tecniche ed organizzative, finalizzate ad un monitoraggio costante del rischio cui le loro infrastrutture informatiche sono potenzialmente esposte [36], ma richiede anche una tempestiva notifica al CSIRT degli eventuali incidenti aventi un impatto sui beni ICT relativi alle proprie reti o ai propri sistemi informativi identificati come parte del Perimetro [37]. Anche in questo caso, a fronte del mancato rispetto degli obblighi in questione, sono previste significative sanzioni amministrative, anche pecuniarie, a carico dei soggetti inadempienti [38].

Dunque, una disciplina che sembra in parte seguire il modello della normativa NIS, con la previsione di specifici obblighi, dei connessi controlli e di eventuali sanzioni in caso di inadempienza. Tuttavia, come abbiamo visto, la

---

[35] In questo senso, espressamente, l'art. 2, comma 1, del d.p.c.m. n. 131/2020. In base al successivo art. 3, «ai fini dell'inclusione nel perimetro, sono oggetto di individuazione […], fatta salva l'estensione ad altri settori […], i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività […]: 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».

[36] Come, ad esempio, predisporre e aggiornare (almeno una volta all'anno) l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, formato sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto dei diversi settori di attività, procedendo ad una valutazione del rischio connesso ai singoli beni così individuati (cfr. l'art. 1, comma 2, lett. b), del d.l. n. 105/2019, nonché l'art. 7 del d.p.c.m. n. 131/2020).

[37] Sulla base di quanto previsto dall'art. 1, comma 3, lett. a) del d.l. n. 105/2019, così come attuato dal successivo d.p.c.m. n. 81/2021, il quale ha distinto tra notifiche obbligatorie (art. 3) e notifiche volontarie (art. 4). Da ultimo, il d.l. n. 115/2022, ha esteso gli obblighi di notifica anche in caso di incidenti riguardanti *asset* che, sebbene non riguardanti direttamente il PSNC, siano comunque di pertinenza dei soggetti in esso ricompresi (vedi l'attuale art. 1, comma 3-*bis*, del d.l. n. 105/2019).

[38] Cfr. l'art. 1, commi 9 ss., del d.l. n. 105/2019.

regolamentazione del PSNC non si sostituisce, ma si affianca a quella delle Direttive NIS e NIS 2, cosa che ha creato diversi problemi di coordinamento, dal momento che le Autorità competenti, gli strumenti di intervento ed i soggetti coinvolti non sono sempre i medesimi [39]. Di qui, a ben vedere, l'urgenza di un intervento normativo finalizzato a dare maggiore coerenza all'architettura nazionale in materia di cybersicurezza, anche per garantire una maggiore efficacia di fronte all'aumento esponenziale della minaccia informatica.

Al momento, però, non sembra che questa sia la strada intrapresa dal legislatore, se solo si pensa a quanto previsto dalla già citata l. n. 90/2024. Con tale provvedimento legislativo, infatti, si sono sostanzialmente anticipati nei confronti delle pubbliche amministrazioni espressamente indicate [40], molti dei contenuti della Direttiva NIS 2 (che sarebbe stata attuata pochi mesi dopo dal già citato d.lgs. n. 138/2024), circostanza che sottolinea ancora una volta la necessità di una maggiore organicità di intervento, vista anche la delicatezza della materia, al fine di evitare potenziali duplicazioni e sovrapposizioni tra procedure che si sono via via stratificate nel corso degli ultimi anni. In ogni caso, appare particolarmente significativa la previsione dell'obbligo, per le pubbliche amministrazioni in questione, di individuare un'apposita struttura organizzativa in materia di cybersicurezza, al cui vertice viene posto il c.d. referente per la sicurezza, soggetto responsabile dell'ufficio e dotato di specifiche competenze tecniche e professionali [41].

---

[39] Anche per questo, come noto, non sono mancati interventi di coordinamento tra le due discipline; si veda, da ultimo, quanto ora ribadito dall'art. 43, comma 2, lett. b), del d.lgs. n. 138/2024, il quale prevede che le notifiche di incidente dei soggetti ricompresi nel PSNC, e i quali ricadano contemporaneamente nell'ambito di applicazione della normativa NIS, assolvono anche agli obblighi di notifica di incidente previsti da quest'ultima. Come noto, infatti, la normativa relativa al PSNC stabilisce termini temporali per la notifica molto più ristretti: 6 ore o, addirittura, 1 ora a seconda della tipologia di incidente (cfr. l'art. 3, comma 4, del d.p.c.m. n. 81/2021).

[40] Per l'individuazione delle quali si veda l'art. 1 della l. n. 90/2024. In ogni caso, tali amministrazioni ricadono oggi tutte anche nel campo di applicazione della già citata Direttiva NIS 2 (si vedano, in particolare, gli Allegati III e IV del d.lgs. n. 138/2024 i quali indicano, tra l'altro, gli organi costituzionali e di rilievo costituzionale, la Presidenza del Consiglio ed i Ministeri, le Regioni, le Province autonome, le Città metropolitane e i Comuni con più di 100.000 abitanti).

[41] Cfr. l'art. 8 della l. n. 90/2024. Tuttavia, il fatto che la legge in questione preveda espressamente una clausola di invarianza finanziaria (art. 24, comma 1), unitamente all'esplicita previsione che «la struttura e il referente […] possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione digitale» già previsti dal Codice dell'amministrazione digitale, di cui al d.lgs. n. 82/2005, non fa ben sperare quanto all'implementazione della previsione in questione.

3. L'Agenzia per la cybersicurezza nazionale e il ruolo della Presidenza del Consiglio dei ministri. I rapporti con il Sistema di informazione per la sicurezza della Repubblica

Al cuore della *governance* nazionale della *cybersecurity*, è posta l'Agenzia per la cybersicurezza nazionale (ACN), istituita dal d.l. n. 82/2021 [42]. La scelta di istituire un organismo specifico per coordinare i diversi attori operanti in questo delicato settore, a ben vedere, sembra rispondere a due necessità di fondo: da un lato, superare il disorganico quadro normativo precedentemente in vigore, con una moltiplicazione di soggetti ed una non sempre chiara ripartizione di competenze, in molti casi ad alto contenuto tecnico; dall'altro, svincolare la gestione della sicurezza cibernetica dall'apparato di *intelligence*, cui era stato sostanzialmente affidato (come abbiamo visto) fin dalla l. n. 133/2012, con tutti i problemi legati alla gestione delle attività di vigilanza, certificazione e controllo che coinvolgono anche soggetti privati, oltre che ai delicati rapporti con le eventuali indagini dell'Autorità giudiziaria [43].

---

[42] Sul punto, cfr. F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 2022, n. 12, p. 241 ss.; I. FORGIONE, *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 R. Ursi (a cura di), *op. cit.*, p. 95 ss.; nonché, volendo, T.F. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2024, n. 2, p. 287 ss.

[43] In tal senso, si veda quanto stabilito dall'art. 17, comma 4, del d.l. n. 82/2021, in base al quale «il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale», essendo pertanto tenuto alla trasmissione delle notifiche di incidente ricevute al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) della Polizia di Stato. Inoltre, è previsto anche che «l'Agenzia trasmette al Procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti» ai fini dell'esercizio delle sue funzioni, *ex* art. 371-*bis* c.p.p. (così l'art. 17, comma 4-*bis*, del medesimo d.l., così come modificato dal d.l. n. 105/2023). Da ultimo, la già citata l. n. 90/2014 ha ulteriormente specificato le forme di doverosa collaborazione tra ACN, forze di polizia e autorità giudiziaria prevedendo, tra l'altro, che, in relazione ad attacchi ai danni di sistemi informatici di cui all'art. 371-*bis*, comma 4-*bis*, c.p.p., o che interessino i soggetti inclusi nel PSNC o quelli ricompresi ambito NIS, l'Agenzia informi «senza ritardo» il Procuratore nazionale antimafia e antiterrorismo. Parallelamente, e quasi specularmente, quando il pubblico ministero acquisisce la notizia di delitti di cui al già citato art. 371-*bis*, comma 4-*bis*, c.p.p., ne deve dare «tempestiva informazione» all'ACN, contemperando lo svolgimento delle attività di indagine con le azioni avviate dall'Agenzia «a fini di resilienza» nell'ambito delle sue competenze; tuttavia, se necessario, può disporre il differimento di uno o più delle predette attività dell'ACN per evitare un grave pregiudizio per il corso delle indagini (cfr., l'art. 22 della l. n. 90/2014, nel modificare l'art. 17 del d.l. n. 82/2021). Sul punto, si vedano F.N. RICOTTA, *Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'autorità giudiziaria*, in *Diritto penale contemporaneo*, 2023, n. 1, p 97 ss.; nonché A. PUGLIESE-G. LASAGNI,

Tuttavia, alla luce della rilevanza strategica della cybersicurezza, il provvedimento legislativo in questione ha confermato, ancora una volta, il ruolo centrale della Presidenza del Consiglio dei ministri cui spetta, in via esclusiva, «l'alta direzione e la responsabilità generale delle politiche di cybersicurezza», l'adozione della relativa «strategia nazionale», vero e proprio documento programmatico fondamentale in materia [44], oltre che la nomina e la revoca del Direttore generale e del Vice Direttore generale della stessa ACN, previa deliberazione del Consiglio dei ministri [45]. Alla luce di questo suo ruolo, il Presidente del Consiglio può impartire specifiche direttive in materia di cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione ed il funzionamento dell'ACN [46]. Al di fuori delle funzioni che gli spettano in via esclusiva, è previsto che egli comunque possa delegare i suoi poteri in materia di *cyber security* all'Autorità delegata per la sicurezza della Repubblica [47].

A supporto delle attività della Presidenza del Consiglio, il d.l. n. 82/2021 prevede l'istituzione di un apposito Comitato interministeriale per la cybersicurezza (CIC), «con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza» [48]. La composizione del CIC ben rappresenta l'ampiezza e la trasversalità di tali politiche: oltre al Presidente del Consiglio, infatti, è prevista la partecipazione dei Ministri degli affari esteri, dell'interno, della giustizia, della difesa, dell'economia, dello sviluppo economico (oggi delle imprese), della transizione ecologica (oggi dell'ambiente), dell'università, delle

---

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa, in questo volume.

[44] Sul punto, vedi ora la *Strategia nazionale di cybersicurezza 2022-2026*, con l'annesso *Piano di implementazione*, adottati dal Presidente del Consiglio con d.p.c.m. 17 maggio 2022, i quali individuano tre direttrici generali di azione (protezione degli *asset* strategici nazionali; risposta alle minacce, agli incidenti e alle crisi in ambiente *cyber*; sviluppo sicuro delle tecnologie digitali e della ricerca industriale), cui sono ricondotte ben 82 misure attuative (www.acn.gov.it).

[45] In questo senso, l'art. 2, comma 1, del d.l. n. 82/2021.

[46] Cfr. l'art. 2, comma 2, del d.l. n. 82/2021.

[47] Come previsto dall'art. 3 del d.l. n. 82/2021, in riferimento a quanto previsto dall'art. 3 della l. n. 124/2007.

[48] In particolare, il CIC «a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale; b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; c) promuove 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; d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale» (art. 4, comma 2, del d.l. n. 82/2021).

infrastrutture, della transizione digitale (se istituito) [49].

Quanto all'ACN, essa è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, anche se «nei limiti di quanto previsto» dal d.l. stesso. Se, infatti, le elevate competenze tecniche richieste, unitamente alle esigenze di flessibilità nell'esercizio delle funzioni assegnate, sembrano richiamare il modello tradizionale di Agenzia, le esigenze di indirizzo e controllo politico relative a tale delicatissimo settore fanno emergere un evidente rapporto di strumentalità rispetto alle funzioni del Presidente del Consiglio in materia [50]. È, infatti, il Presidente del Consiglio, come abbiamo visto, a nominare i vertici dell'ACN, il cui Direttore generale è suo «diretto referente»; a determinare il fabbisogno finanziario annuo della stessa ACN [51]; ad esercitare la potestà regolamentare quanto all'organizzazione, al personale, alla contabilità e alla gestione delle procedure di appalto dell'ACN (in questi due ultimi casi, su proposta del Direttore generale) [52].

Quanto alle funzioni attribuite, appare evidente il fine del legislatore di individuare nell'ACN il fulcro dell'attuale architettura istituzionale in materia di cybersicurezza, anche attraverso il trasferimento in capo ad essa delle funzioni precedentemente riconosciute in materia ad una molteplicità di soggetti istituzionali differenti: Presidenza del Consiglio, DIS, Ministero dello sviluppo economico, Agenzia per l'Italia digitale (AgID). Si ratta di un complesso di

---

[49] Così l'art. 3, comma 3, del d.l. n. 82/2021, il cui successivo comma 5 stabilisce anche che «Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare».

[50] Il quale è previsto si avvalga dell'ACN per l'esercizio delle sue competenze in materia di cybersicurezza (art. 5, comma 2, d.l. n. 82/2021). Sul punto, si veda L. PARONA, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di diritto amministrativo*, 2021, n. 6, p. 709 ss.

[51] In base a quanto previsto dall'art. 11, comma 1, del d.l. n. 82/2021.

[52] Sul punto, si vedano, rispettivamente gli artt. 6, commi 1 e 3; 12, commi 1 e 8; 11, comma 3; e 11, comma 4, del d.l. n. 82/2021. I relativi regolamenti sono stati adottati con i d.p.c.m. n. 223/2021, 224/2021, 222/2021 e 166/2022. Particolarmente significativa, sul punto, appare la previsione che il regolamento del personale e quello sulle procedure di appalto possano derogare alle disposizioni legislative vigenti, tenuto conte delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico. I regolamenti di organizzazione e di contabilità, a loro volta, sono adottati di concerto con il Ministro dell'economia. Per tutti i regolamenti in questione, poi, è prevista espressamente una procedura in deroga rispetto a quella prevista dall'art. 17 della l. n. 400/1988, con la conseguente esclusione del parere espresso dal Consiglio di Stato. In tutti i casi citati, comunque, deve essere sentito il CIC, è necessario il parere del Comitato parlamentare per la sicurezza della Repubblica (COPASIR), nonché (per il regolamento di organizzazione e per quello del personale) anche quello delle Commissioni parlamentari competenti per materia.

funzioni particolarmente ampio e articolato [53], che può tuttavia essere ricondotto a cinque grandi categorie: a) coordinamento tra i diversi soggetti coinvolti in materia di cybersicurezza, quale Autorità nazionale per la cybersicurezza; b) sviluppo di adeguate capacità preventive e di risposta efficace rispetto ad attacchi ed incidenti informatici; c) certificazione dei prodotti, dei processi e dei sistemi ICT, anche attraverso l'esercizio di poteri di vigilanza, di controllo e sanzionatori; d) cooperazione a livello europeo ed internazionale in materia di cybersicurezza; e) supporto alla ricerca, all'innovazione tecnologica e allo sviluppo delle competenze in materia di cybersicurezza.

In via generale, l'ACN è espressamente definita quale «Autorità nazionale per la cybersicurezza» e, in tale veste, «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» [54]. In questa veste, tra l'altro, predispone la già citata strategia nazionale di cybersicurezza, adottata dal Presidente del Consiglio dei ministri, che ben identifica il ruolo strategico dell'ACN, che deve coordinarsi con le altre Amministrazioni coinvolte in materia: il Ministero dell'interno [55], con particolare riferimento alle forze di polizia e al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) della Polizia di Stato [56], il Ministero della difesa, con particolare riferimento alla difesa

[53] Cfr., in particolare, l'art. 7 del d.l. n. 82/2021. Sul punto, vedi ora anche quanto previsto dall'art. 20 della l. n. 132/2025, in base alla quale ACN e AgID sono designate Autorità nazionali per l'intelligenza artificiale. In particolare, all'ACN, «anche ai fini di assicurare la tutela della cybersicurezza», è affidata la responsabilità di vigilare sui sistemi di intelligenza artificiale, con i connessi poteri ispettivi e sanzionatori, secondo quanto previsto dalla normativa nazionale e da quella dell'UE. L'ACN, inoltre, è responsabile «per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza». Infine, è previsto che entrambe le Agenzie (ciascuna per quanto di competenza) assicurino «l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiali» conformi alla già citata normativa, assicurando al contempo il coordinamento e la collaborazione con le pubbliche amministrazioni e le autorità indipendenti coinvolte.

[54] Così l'art. 7, comma 1, lett. a) del d.l. n. 82/2021.

[55] Di cui vengono espressamente mantenute ferme le attribuzioni in quanto Autorità nazionale di pubblica sicurezza: art. 7, comma 1, lett. a), del d.l. n. 82/2021.

[56] Cfr. l'art. 7-*bis* del d.l. n. 144/2005, in base al quale, il CNAIPIC è l'organo del Ministero dell'interno deputato a garantire «la sicurezza e […] la regolarità dei servizi di telecomunicazione», assicurando «i servizi di protezione informatica delle infrastrutture critiche informatizzate di

cibernetica e al ruolo del Comando delle operazioni in rete (COR) [57]; il Sistema di informazione per la sicurezza della Repubblica, per quanto riguarda la ricerca ed elaborazione informativa in ambiente *cyber* coordinata dal DIS e svolta dalle due Agenzie (AISE ed AISI) [58]; il Ministero degli esteri, in relazione alla cooperazione internazionale in materia di cybersicurezza [59].

Quanto alla garanzia di sicurezza delle reti e dei sistemi informativi e alle misure preventive e di risposta in caso di incidenti informatici, l'ACN è ora individuata come "Autorità nazionale competente e punto di contatto unico" per le finalità di cui alla già citata normativa NIS [60]; parallelamente, come già accennato, il d.l. n. 82/2021 ha previsto il trasferimento in capo all'Agenzia delle competenze della Presidenza del Consiglio, del DIS e del Ministero dello sviluppo economico in materia di PSNC, con gli annessi poteri di vigilanza, controllo e sanzione [61]. Coerentemente con tale scelta, sono stati trasferiti presso l'ACN sia il già citato Centro di valutazione e certificazione nazionale (CVCN) [62] sia il CSIRT nazionale, con particolare riferimento ai menzionati obblighi di notifica degli incidenti informatici [63]. Da ultimo, l'Agenzia

interesse nazionale» individuate con decreto dello stesso Ministero dell'interno (vedi il d.m. 9 gennaio 2008). Sul punto, si veda G. TROMBETTA, *Ministero dell'interno e cybersecurity*, in R. Ursi, *op. cit.*, p. 85 ss.

[57] Istituito il 9 marzo del 2020 alle dipendenze del Capo di Sato Maggiore della Difesa, il COR è responsabile della condotta delle operazioni nel dominio cibernetico, nonché della gestione tecnico-operativa in sicurezza di tutti i sistemi ICT della Difesa.

[58] Ferme restando le competenze del comparto *intelligence* in materia di reti, sistemi informativi e servizi informatici attinenti alla gestione delle informazioni classificate, sulla base di quanto previsto dalla l. n. 124/2007 e dai successivi regolamenti di attuazione (cfr. l'art. 7, comma 1, lett. a), del d.l. n. 82/2021).

[59] Cfr. l'art. 7, comma 1, lett. q) del d.l. n. 82/2021.

[60] In questo senso, vedi l'art. 7, comma 1, lett. d) del d.l. n. 82/2021. Sul punto, vedi anche quanto disposto dalle successive lett. n), n-*bis*), in base alle quale l'ACN «sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT […]. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità» e «svolge 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 informatica o attacchi informatici» (così il testo risultante dalle modifiche introdotte dal d.l. n. 105/2023).

[61] Si veda, in particolare, l'art. 7, comma 1, lett. f), h), i) del d.l. n. 82/2021.

[62] In questo senso l'art. 7, comma 4, del d.l. n. 82/2021.

[63] Cfr. l'art. 7, comma 1, lett. d-*ter*) del d.l. n. 82/2021. Sulla base di tali informazioni, l'ACN "provvede alla raccolta, all'elaborazione e alla classificazione" dei relativi dati, "che sono resi pubblici" nell'ambito della sua relazione annuale (art. 7, comma 1, lett. n-*ter*) del d.l. n. 82/2021).

partecipa alle esercitazioni nazionali ed internazionali riguardanti la simulazione di eventi di natura cibernetica [64].

All'ACN, poi, sono attribuiti importanti compiti di certificazione, essendo individuata quale Autorità nazionale di certificazione ai sensi del già citato Regolamento (UE) n. 2019/881 (c.d. *Cybersecurity Act*) ed assumendo «tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico», comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle prescritte sanzioni [65].

Sul piano della cooperazione sovranazionale, con particolare riferimento all'UE, l'ACN risulta a pieno titolo inserita nella rete europea delle corrispondenti Autorità nazionali NIS, in un continuo confronto con l'ENISA volto al complessivo rafforzamento del livello di cybersicurezza comune europeo. In quest'ottica, l'Agenzia è tenuta a cooperare anche con la già citata rete di CSIRT europei. Più in generale, è previsto che essa possa stipulare accordi «con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza […], ferme restando le competenze del Ministero degli affari esteri», anche mediante il coinvolgimento del settore privato e industriale [66]. Da ultimo, «promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali […], ferme restando le competenze del Ministero degli affari esteri» e garantendo il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza [67].

Infine, quanto alla promozione della ricerca e all'innovazione tecnologica l'ACN «supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore». Sempre in quest'ottica, l'ACN «promuove la formazione […] nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di

---

[64] Sulla base di quanto stabilito dall'art. 7, comma 1, lett. o) del d.l. n. 82/2021, al fine di «innalzare la resilienza del paese».

[65] Cfr. l'art. 7, comma 1, lett. e) del d.l. n. 82/2021. Sul punto, cfr. G.G. CUSENZA, *I poteri dell'Agenzia per la cybersicurezza nazionale: una nuova regolazione del mercato cibernetico*, in R. Ursi, *op. cit.*, p. 123 ss.

[66] In questo senso l'art. 7, comma 1, lett. s) del d.l. n. 82/2021.

[67] Secondo quanto previsto dall'art. 7, comma 1, lett. t) del d.l. n. 82/2021.

apposite convenzioni con soggetti pubblici e privati» [68].

Un fascio di competenze, dunque, molto ampio, e che vede nell'Agenzia uno snodo essenziale dell'attuale governo nazionale della cybersicurezza. Tale ruolo strategico, ancora una volta, è confermato anche dalla previsione (quasi una norma di chiusura) in base alla quale l'ACN «cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale», esprimendo «pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza» [69]. In questo modo, anche alla luce delle sue elevate competenze tecniche, l'ACN è individuata quale interlocutrice privilegiata del decisore politico quanto alla necessaria opera di aggiornamento e revisione della (complessa) normativa di settore.

Pur essendo finalizzato, come già anticipato, ad un superamento del precedente assetto che vedeva le competenze in materia di *cyber security* attratte al comparto *intelligence*, il d.l. n. 82/2021 ci consegna un assetto istituzionale che, inevitabilmente, rimane ancora in parte collegato al Sistema di informazione per la sicurezza della Repubblica [70]. Diversi, sul punto, appaiono i dati rilevanti. In primo luogo, come abbiamo visto, viene confermato il ruolo centrale della Presidenza del Consiglio dei ministri, la quale riveste quindi contemporaneamente il ruolo di «alta direzione» delle politiche di cybersicurezza e di Autorità nazionale per la sicurezza della Repubblica. Tale circostanza è plasticamente confermata anche nella scelta di prevedere, quale eventuale Autorità delegata in materia di cybersicurezza, l'Autorità delegata per la sicurezza della Repubblica.

D'altronde, vengono mantenuti inalterati alcuni rilevanti poteri del Presidente del Consiglio in materia di cybersicurezza anche nell'ambito delle sue funzioni di Autorità nazionale per la sicurezza della Repubblica. Particolarmente evidente, sul punto, è l'art. 5 del d.l. n. 105/2019, in base al quale egli,

---

[68] Da ultimo, vedi l'*Agenda di ricerca e innovazione per la cybersicurezza 2023-2026*, elaborata d'intesa con il Ministero dell'università e della ricerca (www.acn.gov.it). Particolarmente significativa, in questo senso, appare anche l'istituzione presso l'ACN del Centro nazionale di crittografia, nell'ambito delle attività di rafforzamento dell'autonomia industriale e tecnologica del paese, in collaborazione con centri universitari e di ricerca, al fine di conseguire nuove capacità crittografiche, secondo quanto previsto dall'art. 7, comma 1, lett. m-*bis*) del d.l. n. 82/2021 (ferme restando, in ogni caso, le competenze dell'Ufficio centrale per la segretezza nell'ambito delle materie sottoposte a classifica per motivi di sicurezza nazionale (art. 9, l. n. 124/2007).

[69] Così l'art. l'art. 7, comma 1, lett. p) del d.l. n. 82/2021.

[70] Cfr., in questo senso, A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, in *Giornale di diritto amministrativo*, 2021, n. 4, p. 538 ss.; S. Rossa, *Cybersicurezza e pubblica amministrazione*, Napoli, Editoriale Scientifica, Napoli, 2023, in particolare p. 91 ss.

«in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, può […] disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati» [71].

Da ultimo, vedi anche quanto previsto dall'art. 7-*ter* del d.l. n. 144/2005, introdotto dall'art. d.l. n. 115/2022, in relazione alle misure di *intelligence* di contrasto attivo in ambito cibernetico, in base al quale lo stesso Presidente del Consiglio emana specifiche disposizioni per fronteggiare «situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale». Tali disposizioni, in particolare, «disciplinano il procedimento di autorizzazione, le caratteristiche e i contenuti generali delle misure che possono essere autorizzate in rapporto al rischio per gli interessi nazionali coinvolti, secondo criteri di necessità e proporzionalità», prevedendo che dell'attuazione di tali misure siano incaricate le Agenzie di *intelligence*.

A conferma di tali (inevitabili) legami, può essere segnalata la composizione del Nucleo per la cybersicurezza (NC), istituito ora presso l'Agenzia, quale organo di supporto operativo del Presidente del Consiglio nell'ambito della prevenzione e preparazione rispetto ad eventuali situazioni di crisi cibernetica [72]. Il

---

[71] Secondo quanto previsto dalla disposizione in questione, «laddove nelle determinazioni di cui al presente comma sia recata deroga alle leggi vigenti anche ai fini delle ulteriori necessarie misure correlate alla disattivazione o all'interruzione, le stesse determinazioni devono contenere l'indicazione delle principali norme a cui si intende derogare e tali deroghe devono essere specificamente motivate» (in questo senso l'art. 5 del d.l. n. 105/2019, così come modificato dal d.l. n. 21/2022). In relazione a tale ipotesi, spetta poi all'ACN provvedere «sulla base delle attività di competenza del Nucleo per la cybersicurezza […] alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio» (art. 7, comma 1, lett. l), del d.l. n. 87/2021).

[72] Cfr. gli artt. 8 ss. del d.l. n. 82/2021. Tale organismo va sostituire il Nucleo per la sicurezza cibernetica (NSC), previsto fin dal d.p.c.m. 24 gennaio 2013 (oltre che da successivo d.p.c.m. 17 febbraio 2017), istituito prima presso l'Ufficio del Consigliere militare della Presidenza del Consiglio, e successivamente incardinato presso il DIS. Sempre a tali d.p.c.m. si deve, in generale, una definizione di crisi cibernetica quale «situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria» (così l'art. 2). Sul punto, si veda F. SERINI, *op. cit.*, p. 265 ss.

NC, presieduto dal Direttore generale dell'ACN, è composto dal Consigliere militare del Presidente del Consiglio, da rappresentanti del DIS e delle Agenzie di intelligence (AISE ed AISI), oltre che da un rappresentante per ciascuno dei Ministeri coinvolti nel CIC e del Dipartimento della protezione civile [73]. In ogni caso, il NC può sempre essere convocato in composizione ristretta, con la sola partecipazione delle amministrazioni e dei soggetti via via interessati [74]. Il NC, in questo caso, svolge il ruolo di raccordo operativo, e per questo motivo acquisisce, tramite il CSIRT, tutte le comunicazioni relative ad incidenti informatici, valutando se essi «assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri» [75].

Da ultimo, un'ulteriore conferma sembra venire dalla recente riforma della composizione dello stesso Comitato interministeriale per la sicurezza della Repubblica (CISR), attuata dalla l. n. 90/2024 [76]. Infatti, con l'aggiunta del Ministri dell'agricoltura, delle infrastrutture e dell'università, la sua attuale composizione è stata sostanzialmente allineata a quella del già citato Comitato interministeriale per la cybersicurezza (CIC), salvo alcune piccole differenze [77].

---

[73] Si veda quanto previsto dall'art. 8, comma 2, del d.l. n. 82/2021. Tuttavia, di fronte a crisi di natura cibernetica, il NC è integrato (a seconda delle necessità) da un rappresentante del Ministero della salute e del Dipartimento dei Vigili del fuoco. In questo caso, inoltre, alle riunioni «possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati» (art. 10, comma 3, del d.l. n. 82/2021).

[74] In questo senso l'art. 8, comma 4, del d.l. n. 82/2021. Tuttavia, in relazione a «specifiche questioni di particolare rilevanza», tale composizione ristretta può essere «di volta in volta estesa» ad un rappresentante della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia o di uno o più soggetti ricompresi nel PSNC, nonché di eventuali altri soggetti interessati (art. 8, comma 4.1, del d.l. n. 82/2021).

[75] Cfr. l'art. 9, comma 1, lett. f), g), del d.l. n. 82/2021. Una particolare attenzione è data ai «casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi» riguardanti il comparto *intelligence*, le forze di polizia, le strutture della Difesa e le altre amministrazioni coinvolte nel NC (art. 9, comma 1, lett. e), del d.l. n. 82/2021).

[76] Cfr. l'art. 7 della l. n. 90/2024.

[77] Il Ministro dell'agricoltura, infatti, non è componente del CIC, mentre il Ministro dell'innovazione tecnologica (se istituito) non è componente del CISR.

4. La governance della cybersicurezza: problemi e prospettive di un sistema integrato e multilivello

Dunque, un quadro istituzionale particolarmente variegato e complesso, sia in relazione alle fonti normative che la disciplinano [78], sia in relazione ai soggetti che ne sono i protagonisti [79]. Si tratta, come abbiamo visto, di un sistema che non solo coinvolge diverse amministrazioni dello Stato e operatori economici privati, ma risulta anche articolato su più livelli, con particolare riferimento alla dimensione europea e internazionale. Così, in ogni caso, non potrebbe non essere, rappresentando la trasformazione digitale uno degli obiettivi strategici non solo dell'UE, ma anche dei singoli Stati.

Alla luce della sua natura strategica e trasversale, non stupisce che la responsabilità politica venga affidata alla Presidenza del Consiglio dei ministri, nell'ambito della sua tradizionale funzione di direzione della politica generale del Governo, *ex* art. 95 Cost. Tuttavia, si tratta di un ambito che richiede elevate competenze di natura tecnica, capacità di coordinamento e rapidità di intervento, anche alla luce dell'aumento esponenziale del rischio e delle minacce in ambiente *cyber* cui si è assistito negli ultimi anni, anche attraverso l'utilizzo di veri e propri strumenti di natura ibrida [80].

La Presidenza del Consiglio, tuttavia, sembra giocare un ruolo a geometria variabile, inserendosi in moduli procedimentali a collegialità più o meno estesa all'interno del Governo. Se, infatti, le nomine del Direttore generale e del Vice-Direttore è previsto avvengano previa deliberazione del Consiglio dei ministri, quest'ultimo non risulta successivamente coinvolto in nessuna altra scelta strategica in materia di *cyber security*.

Tuttavia, si assiste ad un recupero di (pur parziale) collegialità grazie alle rilevanti attribuzioni del già citato Comitato interministeriale per la cybersicurezza (CIC) il quale, nell'ambito delle sue funzioni di consulenza, proposta e

---

[78] In relazione alle quali sarebbe auspicabile un'opera di riordino e di semplificazione. Per la recente proposta di adottare un codice in materia di cybersicurezza, vedi ora E. LONGO, *Il diritto costituzionale e la cybersicurezza*, cit., p. 344.

[79] Sul punto, tra gli altri, A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Rivista Gruppo di Pisa*, 2021, n. 3, p. 529 ss.; F. GAGGERO, *L'azione normativa del Governo in materia di cybersecurity*, in F. BAILO-M. FRANCAVIGLIA (a cura di), *Bilanci e prospettive attorno ai poteri del Governo*, Napoli, Jovene, 2023, p. 347 ss.; F. SANCHINI, *Sicurezza cibernetica e architettura istituzionale: verso una governance costituzionalmente orientata?*, in *Federalismi.it*, 2025, n. 26, p. 170 ss.

[80] Si pensi, solo per fare un esempio, all'utilizzo sempre più evidente di *fake news* nell'ambito di vere e proprie campagne strategiche di disinformazione, attraverso l'utilizzo della rete e dei *social networks*, al fine di inquinare il dibattito pubblico e di influenzare le dinamiche democratiche interne.

vigilanza, (tra l'altro) propone gli indirizzi generali delle politiche di cybersicurezza e vigila sull'attuazione della strategia nazionale in materia [81]. Il Comitato, inoltre, deve essere sentito prima dell'adozione dei diversi d.p.c.m. attuativi previsti dal d.l. n. 82/2021 [82], oltre che proporre alcuni dei più importanti regolamenti previsti dal d.l. n. 105/2019, in materia di Perimetro di sicurezza nazionale cibernetica (PSNC) [83]. Sempre in relazione al PSNC, il Comitato ha il compito di proporre al Presidente del Consiglio il già citato provvedimento amministrativo (segretato) che individua i soggetti rientranti all'interno del Perimetro stesso, oltre che i relativi aggiornamenti [84]. Il CIC, infine, deve esprimere il proprio parere anche sul bilancio preventivo e consuntivo adottati ogni anno dal Direttore generale e approvati con d.p.c.m. [85].

Tuttavia, di fronte a situazioni di crisi che coinvolgono aspetti di cybersicurezza rilevanti per la sicurezza nazionale, qualora il Presidente del Consiglio decida, invece, di convocare il Comitato interministeriale per la sicurezza della Repubblica (CISR), è previsto che alle sedute debba partecipare anche il Direttore generale dell'ACN [86]. Ogni volta che il Presidente del Consiglio attivi il comparto *intelligence*, però, emergono tutti i tratti di "ministerialità" che caratterizzano da sempre le sue rilevanti competenze in materia di sicurezza nazionale, e le forme di (parziale) collegialità risultano conseguentemente più limitate. Si vedano, ad esempio, i già citati casi del potere di disattivazione di apparati o prodotti informatici impiegati nelle reti «in presenza di un rischio grave e imminente per la sicurezza nazionale», che pure avviene previa deliberazione del CISR (*ex* art. 5, d.l. n. 105/2019); o dell'autorizzazione di specifiche 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», per le quali deve comunque essere acquisito il parere del CISR (*ex* art. 7-*ter* del d.l. n. 174/2015) [87].

---

[81] Particolarmente significativo, in questo senso, appare il fatto che le funzioni di Segretario del CIC sono svolte dallo stesso Direttore generale dell'ACN (cfr. l'art. 4, comma 4, del d.l. n. 82/2021).

[82] Con particolare riferimento ai già citati regolamenti di organizzazione interna, del personale, di contabilità e sulle procedure di appalto dell'ACN.

[83] Tale previsione, a ben vedere, è la conseguenza diretta delle modifiche di cui al d.l. n. 82/2021, il cui art. 4, comma 6, prevede che il CIC «svolge […] le funzioni già attribuite al Comitato interministeriale per la sicurezza della Repubblica (CISR)» dal d.l. n. 105/2019, «fatta eccezione per quelle previste dall'art. 5» del medesimo d.l.

[84] Cfr. l'art. 1, comma 2-*bis*, del d.l. n. 105/2019.

[85] Come previsto dall'art. 11, comma 3, lett. a), del d.l. n. 82/2021, il quale prevede anche che debbano essere successivamente trasmessi alla Corte di conti.

[86] In questo senso l'art. 10, comma 1, del d.l. n. 82/2021, il quale prevede anche la partecipazione del Ministro dell'innovazione tecnologica, se istituito.

[87] Significativo, in quest'ultimo caso, l'espresso rinvio alle disposizioni in materia di garanzie funzionali degli addetti ai Servizi di informazione (artt. 17 ss. della l. n. 124/2007).

Tale assetto, più in generale, risulta confermato anche dal ruolo sostanzialmente strumentale assunto dall'ACN in relazione alle competenze della Presidenza del Consiglio in materia di cybersicurezza.

Proprio per questo, l'attuale architettura istituzionale prevede specifiche forme di controllo parlamentare [88], le quali tuttavia vengono rimesse, per lo più, al già citato Comitato parlamentare per la sicurezza della Repubblica (COPASIR), tradizionalmente competente a vigilare sull'attività dei servizi di informazione e sulla gestione del segreto di Stato da parte della Presidenza del Consiglio dei ministri.

È, infatti, a tale Comitato, ad esempio, che il Presidente del Consiglio deve comunicare non solo il più volte citato provvedimento amministrativo (ed i successivi aggiornamenti) con cui vengono individuati i soggetti inclusi nel PSNC [89], ma anche (e preventivamente) le nomine del Direttore generale e del Vice-Direttore dell'ACN (in questo ultimo caso tale comunicazione deve essere fatta anche alle Commissioni parlamentari competenti) [90]. Parallelamente, il COPASIR può chiedere l'audizione del Direttore generale stesso «su questioni di propria competenza», ai sensi dell'art. 31, comma 3, della l. n. 124/2007 [91].

Sempre in relazione ad aspetti significativi dell'organizzazione interna e delle attività dell'Agenzia, è previsto che il COPASIR debba esprimere un parere sui regolamenti di organizzazione, del personale, di contabilità e sulle procedure di appalto dell'ACN; sui primi due, in aggiunta, è prevista anche l'acquisizione del parere «delle Commissioni parlamentari competenti per materia e per i profili finanziari». Uno schema sostanzialmente analogo è previsto in relazione ad alcuni dei d.p.c.m. attuativi del PSNC, che devono essere trasmessi non solo al COPASIR, ma anche alle Commissioni parlamentari competenti per materia, le quali devono esprimere il proprio parere [92].

---

[88] Sul punto, si veda O. CARAMASCHI, *La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari*, in *Osservatorio costituzionale AIC*, 2022, n. 4, p. 69 ss.

[89] Cfr. l'art. 1, comma 4-*ter*, del d.l. n. 105/2019, il quale prevede che tale comunicazione debba avvenire «entro dieci giorni dall'adozione».

[90] Come previsto dall'art. 2, comma 3, del d.l. n. 82/2021. Quanto al personale, il successivo art. 12, comma 5, stabilisce che «dei provvedimenti adottati in materia di dotazione organica dell'Agenzia è data tempestiva e motivata comunicazione alla Commissioni parlamentari competenti e al COPASIR».

[91] Cfr. l'art. 5, comma 6, del d.l. n. 82/2021. Particolarmente significativo, in questo caso, il riferimento alla disposizione della l. n. 124/2007 che stabilisce che il COPASIR «può […] ascoltare ogni altra persona non appartenente al Sistema di informazione per la sicurezza in grado di fornire elementi di informazione o di valutazione ritenuti utili ai fini dell'esercizio del controllo parlamentare», quasi a voler ribadire (ancora una volta) la collocazione dell'ACN al di fuori del comparto *intelligence*.

[92] Secondo quanto previsto dall'art. 1, comma 4-*bis*, del d.l. n. 105/2019, con particolare

Ulteriore profilo, particolarmente delicato, attiene alla gestione del bilancio interno dell'ACN la quale, come abbiamo già visto, gode (tra l'altro) di autonomia contabile e finanziaria. Il d.l. n. 82/2021, infatti, prevede non solo che il Presidente del Consiglio debba previamente comunicare al COPASIR lo stanziamento annuale di risorse assegnate all'ACN [93], ma anche che debba essergli trasmesso (oltre che alle Commissioni parlamentari competenti) il bilancio consuntivo dell'Agenzia, unitamente alla relazione della Corte dei conti [94].

Quanto ai più generali obblighi di comunicazione al Parlamento, è previsto che il Presidente del Consiglio debba trasmettere annualmente alle Camere una Relazione sull'attività svolta dall'ACN nell'anno precedente [95]. Parallelamente, è previsto l'invio, da parte dello stesso Presidente del Consiglio, di un'altra relazione, questa volta diretta al COPASIR, ma relativamente «agli ambiti concernenti la tutela della sicurezza nazionale nella spazio cibernetico» [96].

Da ultimo, anche l'esercizio dei poteri del Presidente del Consiglio in materia di cybersicurezza più strettamente connessi con la tutela della sicurezza nazionale, e coinvolgenti quindi il comparto *intelligence*, prevede la necessità di un controllo da parte del COPASIR. Infatti, sia i provvedimenti di disattivazione, di cui all'art. 5 del d.l. n. 109/2015, sia le misure di contrasto in ambito cibernetico, di cui all'art. 7-*ter* del d.l. n. 174/2015, devono essere comunicati, rispettivamente, entro trenta giorni dalla loro adozione o dalla data di conclusione delle relative operazioni [97].

In conseguenza di tali previsioni, l'attenzione del COPASIR alla cybersicurezza è andata progressivamente aumentando negli ultimi anni, come dimostrato anche dall'esame delle Relazioni periodiche approvate nelle ultime legislature,

---

riferimento ai già citati d.p.c.m. n. 131/2020, sui criteri generali di individuazione dei soggetti inclusi nel PSNC, e d.p.c.m. n. 81/2021, in materia di notifica degli incidenti informatici rilevanti.

[93] Come stabilito dall'art. 11, comma 1, del d.l. n. 82/2021.

[94] Cfr. l'art. 11, comma 3, lett. b) del d.l. n. 82/2021.

[95] Il termine previsto è quello del 30 aprile di ogni anno (cfr. l'art. 14, comma 1, del d.l. n. 82/2021). Da ultimo, vedi la già citata *Relazione* per le attività svolte nel 2024 (Doc. CCXVIII, n. 4; presentata il 5 maggio 2025), www.acn.gov.it; www.parlamento.it.

[96] In questo senso l'art. 14, comma 2, del d.l. n. 82/2021, il quale prevede come termine di presentazione il 30 giugno di ogni anno.

[97] Cfr. quanto previsto dall'art. 5, comma 1-*bis*, del d.l. n. 109/2019 e dall'art. 7-*ter*, comma 4, del d.l. n. 174/2015 (che rinvia all'art. 33, comma 4, della l. n. 124/2007). Da ultimo, si segnala come, in occasione della Relazione del 2024, il COPASIR abbia confermato che, dall'entrata in vigore dell'ultima disposizione citata (introdotta dal già d.l. n. 115/2022), «non risultano essersi verificate le condizioni per l'attivazione di tali misure» (Doc. XXXIV, n. 3, p. 8) www.parlamento.it.

che ormai contengono una parte specificamente dedicata alla cybersicurezza [98]. Il COPASIR, parallelamente, ha deciso di svolgere anche alcuni approfondimenti in materia, attraverso lo svolgimento di apposite indagini conoscitive, indicando puntualmente la necessità di interventi normativi volti a rafforzare la sicurezza cibernetica nazionale, spesso accolti dal legislatore [99]. Da ultimo, alla luce dell'istituzione dell'ACN, il Comitato ha tuttavia segnalato la necessità di una maggiore definizione dei rapporti con il Sistema dei informazione per la sicurezza della Repubblica, anche per evitare possibili sovrapposizioni [100], le quali attualmente rischiano di manifestarsi anche sul piano della stessa attività di controllo parlamentare, vista la necessità di assicurare un coordinamento efficace tra il COPASIR e le Commissioni parlamentari permanenti competenti, più volte evocate.

Il tema, più in generale, richiede un'attenta riflessione in vista delle prospettive di riforma della *governance* in materia di sicurezza nazionale la quale, come abbiamo visto, ha subito forti sollecitazioni negli ultimi anni anche alla luce dell'evoluzione delle stesse minacce presenti nell'arena globale, che impongono un continuo aggiornamento dei protagonisti, delle politiche, degli assetti e delle concrete azioni operative. In questo senso, da ultimo, si riaffaccia l'annosa questione dell'istituzione, nell'ordinamento italiano, di un vero e proprio Consiglio di sicurezza nazionale, che potrebbe rappresentare il fulcro di elaborazione delle politiche e delle azioni a tutela della sicurezza nazionale e degli interessi strategici del paese, direttamente collegato alla Presidenza del Consiglio dei ministri, e la cui introduzione porterebbe non solo ad una complessiva rivisitazione degli attuali Comitati interministeriali competenti in materia (CISR e CIC), ma anche ad un parziale ripensamento del ruolo dello stesso Consiglio

---

[98] Si vedano, in particolare, la Relazione del 2017, approvata sul finire della XVII Legislatura (Doc. XXXIV, n. 5), tutte le Relazioni approvate nel corso della XVIII Legislatura (Doc. XXXIV, nn. 4, 8 e 12), nonché le Relazioni del 2023 e del 2024, approvate nella XIX Legislatura, attualmente in corso (Doc. XXXIV, nn. 1 e 3) www.parlamento.it.

[99] In questo senso, in particolare, si ricordano la *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, approvata il 7 luglio 2010 (XVI Legislatura, Doc. XXXIV, n. 4) nonché, da ultimo, la *Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale*, approvata l'11 dicembre 2019 (XVIII Legislatura, Doc. XXXIV, n. 1), www.parlamento.it.

[100] Cfr., in particolare, la *Relazione sull'attività svolta dal 1° gennaio 2021 al 9 febbraio 2022*, secondo la quale, alla luce della natura sempre più ibrida che le minacce alla scurezza nazionale stanno assumendo nell'attuale scenario, «appare opportuna una rivisitazione della l. n. 124/2007 per una armonizzazione e una più lineare definizione di perimetri e competenze dei diversi soggetti coinvolti nella tutela della sicurezza nazionale nel dominio cibernetico e delle relative funzioni di controllo che il Comitato parlamentare per la sicurezza della Repubblica è chiamato a svolgere» (XVIII Legislatura, Doc. XXXIV, n. 8, p. 42), www.parlamento.it.

supremo di difesa (CSD), presieduto dal Capo dello Stato.

In attesa di tali problematici orizzonti, almeno quanto alla cybersicurezza, è senza dubbio sul piano della capacità di svolgere un efficace ruolo di coordinamento della complessa architettura istituzionale in materia che si gioca gran parte del futuro dell'ACN, al crocevia tra coordinamento multilivello con l'UE e integrazione interna tra i diversi soggetti (pubblici e privati) coinvolti, a vario titolo, nel perimetro di sicurezza nazionale cibernetica [101]. Tra questi, come abbiamo visto, acquistano un ruolo fondamentale anche gli operatori economici nei settori considerati strategici, con i quali l'ACN dovrà promuovere adeguati strumenti di partenariato pubblico-privato, al fine di garantire non solo la sicurezza cibernetica nazionale, ma anche per rafforzare l'autonomia industriale, tecnologica e scientifica dell'Italia nel contesto europeo e internazionale [102].

[101] La necessità di una più stretta collaborazione delle amministrazioni pubbliche con l'Agenzia è stata ribadita dalla Direttiva del Presidente del Consiglio del 6 luglio 2023, con particolare riguardo alla gestione di incidenti di natura informatica. Sul punto, vedi anche quanto stabilito dall'art. 5, comma 5, del d.l. n. 82/2021, il quale prevede che l'ACN possa concludere accordi di collaborazione con «altri organi dello Stato» e «altre amministrazioni» per lo svolgimento dei suoi compiti istituzionali (si vedano ad esempio, i protocolli firmati nel 2023 con la Camera dei deputati e il Senato della Repubblica; per la collaborazione con il Garante per la protezione dei dati personali, in ogni caso, vedi anche l'art. 7, comma 5, del medesimo d.l.).

[102] Sul punto, appare particolarmente significativa la previsione in base alla quale l'ACN partecipa, «per gli ambiti di competenza», al Gruppo di coordinamento in merito all'esercizio dei poteri speciali da parte del Governo nell'ambito dei settori strategici (c.d. *golden power*); cfr. l'art. 7, comma 1, lett. g), del d.l. n. 82/2021.

Capitolo 4

La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello *jus ad bellum*

Giulia Gabrielli [*]

Abstract: Negli ultimi anni, gli attacchi informatici contro le infrastrutture critiche hanno registrato una costante crescita in termini di frequenza e sofisticazione. La vulnerabilità di settori ritenuti essenziali per il funzionamento dello Stato e la popolazione, come la sanità o la fornitura elettrica, a operazioni informatiche ostili è stato oggetto di crescente attenzione in molteplici iniziative a livello internazionale, specialmente rispetto ai rischi e alle minacce che esse comportano per la pace e la sicurezza internazionali. Sebbene l'applicabilità del diritto internazionale al cyberspazio sia ormai pressoché universalmente accettata, permangono tuttora ampie aree grigie rispetto all'attribuzione di attività cibernetiche, oltre che alla qualificazione di determinate operazioni informatiche quali violazioni di norme internazionali. Il presente contributo si propone di contribuire a tale discussione esaminando il tema delle *cyber* operazioni ostili contro infrastrutture critiche dalla prospettiva dello *jus ad bellum*, alla luce dei negoziati in seno all'ONU, nonché delle posizioni ufficiali degli Stati sul diritto internazionale e il cyberspazio.

Keywords: Uso della forza – Cyberspazio – Carta delle Nazioni Unite – Attacchi informatici – *Jus ad bellum* – *Jus contra bellum*

---

[*] Assegnista di ricerca in diritto internazionale presso il Dipartimento di Studi Internazionali, Giuridici e Storico-Politici, Università degli Studi di Milano Statale, giulia.gabrielli@unimi.it.
Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

Tra il 2020 e il 2021, una serie di *ransomware* ha preso di mira alcune strutture ospedaliere in diverse città in Europa e negli Stati Uniti, bloccando l'accesso ai dati e alle reti con l'obiettivo presunto di ottenere un profitto economico in cambio di un riscatto. Le conseguenze di tali azioni sono state varie: dall'esfiltrazione o distruzione di dati, al rinvio di procedure mediche urgenti, fino alla morte di un neonato, presumibilmente a causa dell'indisponibilità immediata di attrezzature essenziali [1].

Più recentemente, tra luglio e settembre 2022, l'Albania è stata bersaglio di *cyber* attacchi che hanno preso di mira molteplici siti web e servizi digitali governativi, con il fine presunto di esfiltrare dati, paralizzare i servizi pubblici e distruggere sistemi e archivi statali, alimentando, così, l'insicurezza nel paese. La paternità delle operazioni, denominate *Homeland Justice*, è stata presto attribuita ad alcuni gruppi di cybercriminali riconducibili all'Iran, il quale ha tuttavia negato qualsivoglia coinvolgimento. In risposta agli attacchi, e in ragione del loro potenziale distruttivo, il governo albanese avrebbe valutato la possibilità di invocare la legittima difesa collettiva, ai sensi dell'art. 5 del Patto Atlantico, trattato istitutivo della NATO, per poi abbandonarla a favore di sanzioni diplomatiche, le prime (note) mai adottate in reazione a operazioni informatiche [2].

Sebbene rappresentativi, gli esempi sin qui menzionati non colgono appieno la reale entità degli attacchi informatici contro settori ritenuti critici o vitali, che negli ultimi anni hanno registrato una costante crescita in termini di frequenza e sofisticazione. All'intensificarsi delle operazioni ascrivibili al fenomeno del cybercrimine, che costituisce la gran parte degli incidenti *cyber* noti, si sono affiancati i recenti conflitti in Ucraina e nel Medio Oriente, i quali hanno contribuito al progressivo dispiegamento di capacità cibernetiche offensive da parte degli Stati, o a essi riconducibili, a supporto di attività di tipo ideologico o di disinformazione, cyber-intelligence, o "*cyber-warfare*" [3].

---

[1] Si vedano: Springhill Medical Center ransomware attack (2019); Brno University Hospital ransomware attack (2020); Ireland's Health Service Executive ransomware attack (2021), in https://cyberlaw.ccdcoe.org.

[2] V. *Letter dated 7 September 2022 from the Permanent Representative of Albania to the United Nations addressed to the Secretary-General and the President of the Security Council*, 9 settembre 2022, A/76/943-S/2022/677. Per una discussione nel merito della liceità delle operazioni, si veda A.L. SCIACOVELLI, *Taking cyberattacks seriously: the (likely) Albanian cyber aggression and the Iranian responsibility*, Working paper, 2023.

[3] CLUSIT, *Rapporto 2024 sulla Sicurezza ICT in Italia*, 2024, in https://clusit.it, p. 10; R. ALLEGRI-G. SCICHILONE, *Il dominio cyber negli attuali scenari di guerra mediterranei: il caso del conflitto in Medio Oriente*, nel presente volume.

Uno sviluppo preoccupante in questo senso riguarda la crescente tendenza a individuare beni e servizi essenziali per la popolazione, specialmente relativi alla sanità pubblica, oltre che sistemi governativi e militari, quali obiettivi di *cyber*-operazioni [4], con la conseguente accresciuta vulnerabilità ad attività malevole condotte da una vasta gamma di autori, non limitatamente agli Stati e ai loro organi, ma anche e soprattutto da gruppi terroristici, gruppi armati non statali e, a vario titolo, individui [5].

Le potenziali vulnerabilità di infrastrutture ritenute vitali per il funzionamento degli Stati ha rappresentato un tema trasversale nelle molteplici iniziative intraprese in seno a organizzazioni internazionali a carattere universale e regionale volte a discutere le minacce e i potenziali rischi che gli utilizzi malevoli delle tecnologie dell'informazione e della comunicazione (ICT, nell'acronimo inglese) comportano per la sicurezza nazionale e internazionale, nonché le eventuali misure di contrasto e di cooperazione per farvi fronte. Tra queste, spiccano per partecipazione e rilevanza gli sforzi assunti dall'Assemblea Generale delle Nazioni Unite (d'ora in avanti, UNGA) in materia di «sviluppi nel campo delle tecnologie dell'informazione e delle comunicazioni nel contesto della sicurezza informatica» [6]. A partire dal 1998, i due principali "binari" di

---

[4] Rapporto Clusit 2024, cit., p. 15 ss. Il Dipartimento della Difesa statunitense definisce genericamente *cyberoperations* l'«*employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace*». L'*Institut de Droit International*, nel tentativo di circoscrivere l'«immensa» gamma di *cyber* attività a disposizione di attori statali e non, indica a titolo di esempio: «*cyber warfare, including both attacks on networks and the use of autonomous weapons systems; remote scientific research over the oceans; the compilation of banks of personal data; the automatization of international sales transactions; the creation of virtual reality communities in which members engage in activities that may be unlawful elsewhere; and the creation of non-State-based international currencies*». DIPARTIMENTO DELLA DIFESA DEGLI STATI UNITI, *DOD Dictionary of Military and Associated Terms*, 2017, in www.tradoc.army.mil; INSTITUT DE DROIT INTERNATIONAL, *Preliminary Report of the 8th Commission on 'The Applicability of International Law to Cyber Activities'*, 2023, in www.idi-iil.org.

[5] A. BUFALINI, *Uso della forza, legittima difesa, e problemi di attribuzione in situazioni di attacco informatico*, in A. LANCIOTTI-A. TANZI (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, Jovene, Napoli, 2012, pp. 406-407. Sulla capacità di attori non statali, come Hamas e Hezbollah, di condurre operazioni informatiche strategiche, più o meno offensive, si veda R. ALLEGRI-G. SCICHILONE, *op. cit.*, p. 11 ss.

[6] J. JOLLEY, *Recommendation 13(f)*, in CIVIL SOCIETY AND DISARMAMENT, *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary*, United Nations Office for Disarmament Affairs, New York, 2017, p. 169 ss. Per una discussione sulle iniziative in materia di cybersicurezza in ambito ONU, si veda, in generale, P. GARGIULO, *Nazioni Unite,* Cybersecurity *e Diritto Internazionale*, in O. PORCHIA-M. VELLANO (a cura di), *Il diritto internazionale per la pace e nella guerra. Sviluppi recenti e prospettive future. Liber Amicorum in onore di Edoardo Greppi*, Edizioni Scientifiche

negoziazione, il Gruppo di Esperti Governativi (UNGGE) e il Gruppo di lavoro aperto (OEWG), istituiti dall'UNGA, hanno rappresentato per gli Stati la principale piattaforma organizzativa in materia di cybersicurezza [7], influenzando ulteriori discussioni in altri e numerosi *fora*. Degno di nota è il *consensus* raggiunto dagli Stati coinvolti nelle negoziazioni circa alcune "norme" volontarie e non vincolanti volte a promuovere il comportamento responsabile degli Stati nel cyberspazio, le cosiddette *cyber norms*, le quali riconoscono la centralità delle infrastrutture critiche (e delle relative vulnerabilità), individuando alcune misure per assicurarne la protezione da minacce informatiche.

Le negoziazioni multilaterali intraprese in seno ai due gruppi hanno avuto, inoltre, l'indubbio merito di riconoscere e affermare inequivocabilmente la piena applicabilità delle norme e dei princìpi del diritto internazionale al dominio cibernetico [8]. Tale riconoscimento è stato successivamente fatto proprio dall'UNGA e da diversi Stati e organizzazioni internazionali, inclusa l'Unione europea (UE), tramite prese di posizione nazionali o congiunte sul diritto internazionale applicabile al cyberspazio, rese pubbliche a partire dal 2019 [9]. Seppur apparentemente scontata, tale affermazione cela l'annoso dibattito circa l'idoneità del diritto internazionale esistente a regolare un contesto in continua evoluzione, nonché caratterizzato dall'intangibilità e dall'anonimato, come quello digitale. Ai fini di questa breve indagine, partiremo dall'assunto ormai (quasi [10])

Italiane, Torino, 2023; G.M. FARNELLI, *Il contributo delle Nazioni Unite allo sviluppo dell'International Cybersecurity Law*, in *OSORIN Working Paper 1-2020*, pp. 135-138.

[7] M. FINNEMORE-K. SIKKINK, *International norm dynamics and political change*, in *International Organization*, 1998, vol. 52, n. 4, p. 887.

[8] UNGA, A/68/98, 24 giugno 2013 (d'ora in avanti, "UN GGE Report 2013"); UNGA, A/70/174, 22 luglio 2015 (d'ora in avanti, "UN GGE Report 2015"); UNGA, A/76/135, 14 luglio 2021 (d'ora in avanti, "UN GGE Report 2021"); UNGA, A/AC.290/2021/CRP.2, 10 marzo 2021.

[9] Si veda CONSIGLIO DELL'UNIONE EUROPEA, *Declaration on a Common Understanding of International Law in Cyberspace*, 18 novembre 2024, p. 4. La lista delle posizioni degli Stati sull'applicabilità del diritto internazionale al cyberspazio è accessibile all'indirizzo: https://cyberlaw.ccdcoe.org.

[10] Si segnalano posizioni divergenti rispetto alla piena applicabilità del diritto internazionale al cyberspazio, specificatamente riguardo all'esercizio del diritto di legittima difesa in reazione a condotte mediante ICT, al diritto umanitario e alla responsabilità statale, ivi incluse le contromisure, manifestate da alcuni Stati nell'ambito delle negoziazioni del GGE (specialmente Cuba, Cina e Russia). P. GARGIULO, *op. cit.*, pp. 64-65; F. DELERUE-F. DOUZET-A. GÉRY, *The Geopolitical Representations of International Law in the International Negotiations on the Security and Stability of Cyberspace, Report No. 75*, IRSEM/EU Cyber Direct, 2020, in https://eucyberdirect.eu, p. 19. Si veda, inoltre, *Documento de Posición de la República de Cuba Sobre la Aplicación del Derecho Internacional a las Tecnologías de la Información Y Comunicación en el Ciberespacio*, La Havana, 28 giugno 2024.

universalmente condiviso che le norme e i princìpi del diritto internazionale, inclusa la Carta delle Nazioni Unite (d'ora in avanti, CNU) «*in its entirety*» [11], si applicano alle condotte mediante ICT degli Stati o a essi riconducibili (le cosiddette «*State-sponsored cyber operations*») [12] e ne limitano il margine d'azione anche nella "quinta dimensione" della conflittualità [13].

Cionondimeno, *come* tali norme e principi di fatto regolino il comportamento degli Stati è ancora oggetto di acceso dibattito, specialmente rispetto alle soglie e alle circostanze necessarie perché determinate operazioni informatiche possano configurarsi come una violazione di obblighi internazionali, quali il divieto dell'uso della forza, il principio di non intervento e il principio di sovranità. Il presente contributo si propone di contribuire a tale discussione in particolare esaminando il tema delle *cyber* operazioni ostili contro le infrastrutture critiche dalla prospettiva dello *jus ad bellum*, alla luce dei dibattiti intrapresi in seno ai negoziati già brevemente menzionati e delle *cyber norms* ivi concordate, nonché delle posizioni degli Stati sul cyberspazio.

2. La (complessa) questione dell'attribuzione delle *cyber* condotte

Prima di procedere con l'analisi della qualificazione giuridica di talune operazioni informatiche contro infrastrutture critiche, riteniamo opportuno soffermarci brevemente su due questioni di carattere preliminare, ossia l'attribuzione delle condotte *cyber* a uno Stato e la definizione di infrastruttura critica quale oggetto di operazioni informatiche malevole.

In primo luogo, come noto, è l'imputabilità a uno Stato di una condotta informatica a determinare l'applicabilità delle norme e dei principi di diritto internazionale e, nell'eventualità che questa contravvenga a certi obblighi di natura pattizia o consuetudinaria, a implicarne la responsabilità sul piano internazionale [14]. Gli attacchi mediante ICT sollevano il noto e risalente problema di stabilire un collegamento tra l'attacco informatico e uno Stato, specie in considerazione del fatto che essi si verificano tipicamente in forma anonima e non

[11] UN GGE Report 2021, p. 18.

[12] Si veda, ad esempio, F. DELERUE, *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020, p. 13, p. 19 ss.

[13] Si veda: www.globalsecurity.org/military/library/policy/dod/d20050318nms.pdf.

[14] Commissione di Diritto Internazionale, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Supplement No. 10 (A/56/10), chp.IV.E.1, novembre 2001, art. 1-3. Nel caso di condotte di attori non statali non attribuibili allo Stato, queste sarebbero regolate dal diritto interno.

sono apertamente rivendicati [15]. In taluni casi, inoltre, non è da escludersi la possibilità che gruppi di *hacktivisti* agiscano con l'acquiescenza di agenzie governative al fine di conseguire obiettivi di natura più ampia, come la "guerra" psicologica, campagne di disinformazione o sabotaggio [16].

Qualsiasi processo di attribuzione di un'operazione informatica a uno Stato presuppone considerazioni di natura giuridica, tecnica e politica [17], vale a dire l'individuazione del computer utilizzato per lanciare tale operazione (la c.d. attribuzione tecnica), l'identificazione della persona responsabile, ovvero dell'autore materiale della condotta, e – in virtù della sussistenza di un possibile collegamento – l'eventuale coinvolgimento dello Stato [18].

Non è peraltro sufficiente accertare il controllo esclusivo dello Stato sul territorio di provenienza per implicarne la responsabilità sul piano internazionale, neppure qualora l'operazione in questione tragga origine da un'infrastruttura informatica governativa [19]. Secondo gli Esperti del Manuale di Tallinn, difatti, non è infrequente che queste vengano utilizzate per finalità malevole da gruppi *hacker* o da altri Stati che ne abbiano acquisito il controllo [20]. Ciò vale, *a fortiori*, per le operazioni informatiche provenienti da infrastrutture private situate nel territorio di uno Stato: la possibilità di condurre attacchi di tipo *distributed denial of service* (DDoS) tramite reti di dispositivi infettati a insaputa degli

---

[15] A. BONFANTI, *Attacchi informatici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Riv. dir. int.*, 2019, n. 3, p. 710 ss.

[16] Rapporto Clusit 2024, cit., p. 10, p. 290. Un esempio significativo di tale fenomeno è rappresentato dall'intensificarsi, a partire dal 2022, di attacchi informatici ed episodi di sabotaggio fisico nel settore energetico di diversi Stati europei, presumibilmente attribuibili a *hacker* sostenuti dalla Russia, con il presunto scopo di perseguire obiettivi strategici, tra cui la creazione di fratture interne, l'erosione della fiducia nei governi europei e l'indebolimento del sostegno all'Ucraina.

[17] N. TSAGOURIAS, *Cyber attacks, self-defence and the problem of attribution*, in *Journal of Conflict and Security*, 2012, vol. 17, p. 233 ss.

[18] Per un'analisi sull'attribuzione tecnica o fattuale di attacchi informatici, si vedano F. DELERUE, *Cyber operations*, cit., pp. 55-85; A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Edizioni Scientifiche Italiane, Napoli, 2023, pp. 32-63.

[19] A. BONFANTI, *op. cit.*, p. 711 ss.; *Corfu Channel case (United Kingdom c. Albania),* I.C.J. Reports, 1949, p. 18. Si veda, inoltre, UN GGE Rapporto 2015, *op. cit.*, par. 28(f).

[20] M.N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, II ed., Cambridge University Press, Cambridge, 2017, p. 91. Il Manuale di Tallinn, pubblicato nella sua prima edizione nel 2013, è il frutto del lavoro di un gruppo di esperti internazionali riuniti sotto l'egida del *NATO Cooperative Cyber Defence Centre of Excellence*. Benché non sia vincolante, il manuale è considerato particolarmente autorevole in materia di diritto internazionale applicabile al cyberspazio, e diversi Stati ne hanno richiamato alcuni orientamenti nei propri *position paper*.

utenti (le cosiddette *botnet*) di fatto implica che qualsiasi computer, ovunque localizzato, possa essere compromesso e utilizzato per condurre attività ostili [21].

Appurato, quindi, che la mera individuazione del territorio di origine della minaccia informatica non è sufficiente, di per sé, a stabilirne il responsabile, l'operazione tecnico-giuridica volta ad attribuire una determinata condotta allo Stato è un compito di non facile esecuzione, specialmente considerando che il contesto cibernetico vede coinvolti, in larga parte, soggetti privati spesso non inquadrati nell'organizzazione statale [22]. Di norma, laddove un'operazione informatica non possa essere ricondotta a un organo dello Stato, come l'*intelligence*, l'apparato militare o le agenzie di (*cyber*)sicurezza nazionale, o a qualsivoglia individuo o entità che agisca sotto la sua «completa dipendenza [23]», oppure lo Stato non riconosca apertamente come propria tale condotta – in tali casi, questa sarebbe imputabile allo Stato conformemente agli artt. 4 e 11 del progetto di articoli sulla responsabilità dello Stato della Commissione di diritto internazionale (d'ora in avanti, CDI), rispettivamente – si renderebbe necessario dimostrare che gruppi di *hacker* o *hacktivisti* agiscano sotto sue istruzioni, direzione o controllo, ipotesi prevista dall'art. 8 del progetto [24].

Quanto al criterio della direzione o controllo, stando alla tesi maggioritaria adottata dalla Corte internazionale di Giustizia (d'ora in avanti, CIG) nel caso *Nicaragua* del 1986 e successivamente precisata nel caso *Applicazione della Convenzione sul Genocidio* del 2007, nonché sostenuta da alcuni Stati nelle posizioni nazionali sul diritto internazionale nel cyberspazio [25], l'elemento da dimostrare affinché la responsabilità internazionale dello Stato possa essere fatta valere anche per attività di privati è che esso eserciti un «controllo effettivo» su ciascuna delle condotte lesive, incluse mediante ICT, poste in essere da tali gruppi o individui [26].

---

[21] *Ibidem*.

[22] A. STIANO, *op. cit.*, p. 92.

[23] *Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports, 1986*, par. 110; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007*, par. 392-393.

[24] V. *Draft Articles on Responsibility of States*, cit., art. 8; A. BONFANTI, *op. cit.*, p. 712; F. DELERUE, *Attribution to State of Cyber Operations Conducted by Non-State Actors*, in E. CARPANELLI-N. LAZZERINI (a cura di), *Use and Misuse of New Technologies*, Springer, Cham, 2019, p. 236.

[25] Si vedano, ad esempio, le posizioni del Brasile («*for a private person or entity's conduct be attributable to a State, it has to be proved that the state had "effective control" over the operations*»), dei Paesi Bassi e della Norvegia («*[a] State may be held responsible under international law for cyber operations conducted by non-State actors if these are conducted on the direct instructions of the State or under its direction or effective control*»).

[26] COMMISSIONE DI DIRITTO INTERNAZIONALE, *Draft articles on Responsibility of States for*

Ciò detto, in conformità all'art. 8 del progetto di articoli, l'effettivo coinvolgimento dello Stato in operazioni informatiche ostili di qualsivoglia entità o natura andrebbe valutato caso per caso e in base alle circostanze fattuali [27]. Per un verso, uno Stato che si limitasse a fornire un *malware* a un gruppo di *hacker* o a invocare la mobilitazione di *hacktivist* per condurre attacchi imprecisati mediante ICT non potrebbe essere ritenuto responsabile delle azioni di questi ultimi [28]. Per contro, laddove il dipartimento IT di una società privata abbia ricevuto istruzioni a condurre attacchi DDoS contro un determinato obiettivo da parte di uno Stato, tali operazioni sarebbero attribuibili a quest'ultimo [29]. Analogamente, qualora fosse dimostrato che lo Stato detenga il controllo effettivo sull'esecuzione e sullo svolgimento di una determinata operazione informatica da parte di soggetti non statali, e che l'attività da questi svolta costituisca parte integrante di tale operazione [30], o – come nel noto caso di *Stuxnet* [31] – che

Internationally Wrongful Acts, with commentaries, in *Yearbook of the International Law Commission*, 2001, vol. II, art. 8, par. 3; Caso *Nicaragua*, cit., par. 115; A. BONFANTI, *op. cit.*, p. 712; D. MAURI, *"Aggiornamento disponibile": nuove tecnologie, uso della forza e diritto internazionale*, in T. CASADEI-S. PIETROPAOLI, *Diritto e tecnologie informatiche*, Wolters Kluwer-Cedam, 2021, p. 200; M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 96. Si rammenta l'approccio della Camera d'appello del Tribunale penale per la ex Jugoslavia, la quale, in disaccordo con i giudici della CIG, ha formulato un criterio fondato sul controllo globale (o *overall control*) dello Stato sui privati, di fatto ampliando l'ambito di responsabilità dello Stato. *Prosecutor v. Dusko Tadic*, caso n. IT-94-1-A, parr. 98-145; A. CASSESE-M. FRULLI (a cura di), *Diritto internazionale*, IV ed., il Mulino, Bologna, 2021, pp. 378-379.

[27] V. *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, cit., art. 8, par. 5; M.N SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 95.

[28] M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 97; K. MAČÁK, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, in *Journal of Conflict & Security Law*, 2016, vol. 21, n. 3, p. 415.

[29] K. MAČÁK, *op. cit.*, p. 415.

[30] M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 96.

[31] Scoperto dal governo iraniano nel luglio 2010, *Stuxnet* è un *malware* che ha infettato la centrale nucleare di Natanz con lo scopo, presunto, di intralciare il programma nucleare dell'Iran. Il codice, scritto in modo da alterare la velocità di rotazione delle centrifughe per l'arricchimento dell'uranio, ne avrebbe interrotto il funzionamento, presumibilmente causando il guasto di circa un migliaio di esse. Sulla base di alcune caratteristiche tecniche e della sofisticazione del software, *Stuxnet* è stato ricondotto al lavoro congiunto di Israele e Stati Uniti e altri *threat actor*, senza, tuttavia, evidenze concrete circa l'identità degli sviluppatori né i danni effettivi prodotti dall'operazione. Per una discussione su *Stuxnet* e sulle difficoltà di attribuirne la responsabilità, si veda, *ex multis*, D. ALBRIGHT-P. BRANNAN-C. WALROND, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, Institute for Science and International Security, 22 dicembre 2010; R. BUCHAN, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions*, in *Journal of Conflict and Security Law*, vol. 17, n. 2, 2012, p. 219 ss.; A. STIANO, *op. cit.*, pp. 46-51, 148-150.

sussista una «*ongoing relationship of subordination*» tra lo Stato e un gruppo di programmatori coinvolti nello sviluppo di un *software* malevolo, potrebbero prefigurarsi le ipotesi di "direzione e controllo" di cui all'art. 8 del progetto di articoli [32].

3. Le *cyber* operazioni contro le infrastrutture critiche e le norme ONU sul comportamento responsabile degli Stati

Nel trattare il tema della qualificazione di operazioni informatiche ostili contro infrastrutture critiche ci si confronta, in secondo luogo, con un problema di definizioni: la disciplina del diritto internazionale non offre una nozione univoca e universalmente riconosciuta di infrastruttura critica. Nella risoluzione 58/199, "*Creation of a global culture of cybersecurity and the protection of critical information infrastructures*" del 23 dicembre 2003, l'UNGA individuava diversi settori essenziali per gli Stati, inclusi quelli relativi alla generazione, alla trasmissione e alla distribuzione di energia, al trasporto aereo e marittimo, ai servizi bancari e finanziari, al commercio elettronico, all'approvvigionamento idrico, alla distribuzione di cibo e alla salute pubblica. Contestualmente, l'UNGA riconosceva agli Stati la possibilità di determinare quali settori essi stessi reputassero essenziali per la loro sicurezza nazionale – incluse le infrastrutture informatizzate di natura critica (CII) [33], ossia quei sistemi informatici e di rete fondamentali per il funzionamento di uno Stato [34] – e la cui compromissione («*incapacitation*») o distruzione («*destruction*») potrebbe indebolire la sicurezza, l'economia, la salute pubblica o l'ambiente [35].

Alla luce della dipendenza quasi totale delle nostre società ed economie da sistemi o reti di computer, nonché della rilevanza, anche geopolitica, dei dati (inclusa la loro conservazione, fusione o archiviazione), emerge chiaramente come la nozione di infrastruttura critica non si limiti a strutture fisiche tradizionali (si pensi a centrali elettriche, reti di trasporto, ospedali), ma si estenda anche a quelle infrastrutture che sono costituite da sistemi e reti informatiche o che da

[32] K. MAČÁK, *op. cit.*, p. 419.

[33] UN Doc, A/RES/58/199, 30 gennaio 2004.

[34] OECD, *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*, 2008, in https://ccdcoe.org.

[35] La definizione riportata è una traduzione, a cura dell'autrice, della versione originale: «*Physical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment*». M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 564.

essi dipendono in modo vitale [36]. Ciò detto, sarebbe concepibile supporre che attacchi informatici non necessariamente violenti o distruttivi potrebbero causare effetti diretti o indiretti particolarmente gravi, come nel caso dell'interruzione di sistemi bancari o della sospensione prolungata della rete elettrica, con conseguenze rovinose sulla stabilità economica di uno Stato o sulla salute pubblica [37]. Da queste considerazioni discende la duplice dimensione della vulnerabilità: da un lato, quella delle infrastrutture che si appoggiano a sistemi digitali per operare; dall'altro, quella delle infrastrutture digitali che costituiscono esse stesse settori critici, incluse nella loro componente fisica (come i servizi di DNS, *cloud computing* o *data center*; i registri dei nomi di dominio di primo livello; i cavi sottomarini) [38].

Alla luce di quanto sopra, non è dunque un caso che, già dal 2010, quando il secondo GGE raggiunse per la prima volta il *consensus* su un rapporto finale, il tema della vulnerabilità delle infrastrutture critiche fosse centrale. Tre delle cosiddette *cyber norms*, ovvero le norme volontarie e non vincolanti sul comportamento responsabile degli Stati concordate in seno al GGE e successivamente reiterate nelle più recenti iterazioni dell'OEWG, sono espressamente dedicate al tema della protezione delle infrastrutture critiche [39]. Nel recente *Draft Final Report* adottato dal gruppo di lavoro aperto il 25 luglio 2025 si sottolinea come gli Stati «*continued to underline the importance of the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII)*», sottolineando che «*ICT activity that intentionally damages CI or CII or otherwise impairs the use and operation of CI or CII to provide services to the public can also have cascading domestic, regional and global effects [and] poses an elevated risk of harm to the population and can be escalatory*» [40].

In particolare, la norma 13(f), nel considerare i considerevoli effetti che la compromissione di tali infrastrutture potrebbe comportare in termini di vite umane, di impatto sull'economia e sullo sviluppo, dispone che gli Stati non *dovrebbero* condurre o sostenere consapevolmente attività di natura informatica contrarie ai loro obblighi internazionali e intenzionalmente volte a danneggiare

---

[36] F. DELERUE, *Cyber operations*, cit., pp. 302-304; P. TESSARI-K. MUTI, *Resilienza e sicurezza delle infrastrutture critiche nel contesto italiano ed europeo*, in *Istituto Affari Internazionali (IAI)*, 2024, vol. 24, n. 11, pp. 21-22; S. HAATAJA, *Cyber operations against critical infrastructure under norms of responsible state behaviour and international law*, in *International Journal of Law and Information Technology*, 2022, vol. 30, p. 427.

[37] M.C. WAXMAN, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in *The Yale Journal of International Law*, 2011, vol. 36, no. 1, p. 436.

[38] F. DELERUE, *Cyber operations*, cit., pp. 302-304; P. TESSARI-K. MUTI, *op. cit.*, pp. 21-22.

[39] UN GGE Report 2015, cit., p. 8; UN GGE Report 2021, cit., p. 12 ss.

[40] UN Doc A/AC.292/2025/CRP.1, 11 luglio 2025, par. 34(b).

un'infrastruttura essenziale per la fornitura di servizi pubblici o a comprometterne l'utilizzo e il funzionamento [41].

Tale norma, alla stregua delle altre undici *cyber norms* elaborate in seno al GGE, ha sollevato non poche perplessità in dottrina, specificatamente rispetto alla loro portata giuridica ed effettiva capacità di orientare il comportamento degli Stati nel cyberspazio. Per un verso, tali norme hanno indubbiamente aperto la strada a possibili sviluppi normativi in ambito *cyber* a livello internazionale: benché non siano giuridicamente vincolanti per gli Stati, esse sono state adottate per *consensus* nelle varie iterazioni dei lavori del GGE e dell'OEWG, incorporate in una successiva risoluzione dell'UNGA, la quale esortava gli Stati a farsi guidare da esse nelle loro attività mediante ICT, nonché riprese da alcune organizzazioni internazionali al di fuori dell'ONU, inclusa l'UE, a dimostrazione di una certa condivisione dei princìpi ivi delineati [42].

Per altro verso, sebbene alcune di esse si presentino distintamente come raccomandazioni agli Stati, tra cui le misure da attuare a livello domestico per proteggere l'integrità della *supply chain* o la segnalazione di vulnerabilità ICT, altre *cyber norms* non sembrano del tutto avulse da obblighi internazionali già esistenti. Si pensi a quelle che richiamano gli Stati al rispetto dei loro obblighi in materia di diritti umani (norma 13(e)), oppure alla cooperazione per garantire la sicurezza e la stabilità del cyberspazio e a prevenire attività mediante ICT suscettibili di minare la pace e la sicurezza internazionali (norma 13(a)) [43].

A ben vedere, la summenzionata norma 13(f), nel prevedere che gli Stati «*should not conduct or knowingly support ICT activity contrary to [their] obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public*», non introduce un divieto *ex novo*, giacché si limita a reiterare l'applicabilità al mondo digitale di obblighi già esistenti [44]. Essa può

---

[41] UN GGE Report 2013, cit., p. 12. Oltre alla norma 13(f), le norme 13(g) e (h) richiamano espressamente gli Stati alla protezione delle infrastrutture critiche localizzate sul proprio territorio, tramite l'adozione di misure appropriate per rispondere a eventuali minacce ICT, e sul territorio di altri Stati, tramite l'assistenza reciproca in caso di operazioni malevole contro settori critici, incluse quelle provenienti dal proprio territorio. Per una discussione, si veda: M. BERK, *Recommendations 13 (g) and (h)*, in CIVIL SOCIETY AND DISARMAMENT, *op. cit.*, pp. 191-222.

[42] UN Doc. A/RES/70/237, 30 dicembre 2015; UN Doc. A/RES/73/27, 11 dicembre 2018; EUROPEAN COUNCIL, *Council Conclusions on malicious cyber activities*, n. 7925/18, 16 aprile 2018; *ASEAN Leaders' Statement on Cybersecurity Cooperation*, 32nd ASEAN Summit, 27 aprile 2018, in https://asean.org.

[43] M. LEHTO, *The rise of cyber norms*, in N. TSAGOURIAS-R. BUCHAN (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, Cheltenham, 2021, p. 39 ss.

[44] J. JOLLEY, *op. cit.*, p. 174.

infatti essere interpretata come *lex lata* tesa a richiamare il divieto per gli Stati di condurre intenzionalmente, ovvero di supportare volontariamente tramite *proxies*, *hacktivisti* o altri attori non statali, attività che possano danneggiare o compromettere l'utilizzo e il funzionamento di infrastrutture critiche, purché tali attività siano contrarie a obblighi internazionali derivanti dal diritto pattizio o consuetudinario. Da tale lettura, si può dedurre che un'operazione configurabile come uso della forza armata, e quindi integrante la soglia richiesta dall'art. 2, par. 4, della CNU [45], laddove sia sferrata da un organo dello Stato, *de iure* o *de facto*, oppure sotto sue istruzioni, direzione o controllo, e diretta contro un'infrastruttura che lo Stato vittima individua come critica, configurerebbe una violazione sia del divieto dell'uso della forza nelle relazioni internazionali, sia della norma 13(f) [46].

Ciò considerato, poiché la norma in questione richiama apertamente gli obblighi internazionali per gli Stati, riteniamo opportuno muovere la nostra indagine verso l'analisi di quelle norme di diritto internazionale di carattere vincolante che appartengono al c.d. *jus ad bellum*.

4. La disciplina dell'uso della forza nelle relazioni internazionali: cenni introduttivi

A fronte delle potenziali gravi ripercussioni che operazioni informatiche ostili potrebbero comportare per la sicurezza nazionale e internazionale, specialmente quando queste hanno come obiettivo infrastrutture o servizi essenziali per la popolazione, la dottrina internazionalistica si è interrogata a lungo, e secondo alcuni in maniera pressoché esclusiva [47], sulla rilevanza della disciplina

[45] V. *infra*, par. 5.

[46] J. JOLLEY, *op. cit.*, p. 174.

[47] R. BUCHAN, *op. cit.*, p. 221. Va qui chiarito che la discussione sul tema del diritto internazionale applicabile alle cyber condotte statali non è affatto limitato alla dottrina dello *jus ad bellum*, oggetto di questo contributo. Operazioni informatiche ostili potrebbero essere analizzate e interpretate alla luce delle norme sulla responsabilità penale individuale, nel caso del cybercrimine, oggetto della Convenzione di Budapest sulla criminalità informatica del Consiglio d'Europa del 23 novembre 2001. Inoltre, esse potrebbero qualificarsi – a seconda delle circostanze e delle conseguenze – quali violazioni dei principi di sovranità e/o di non ingerenza negli affari interni o esterni di un altro Stato. In caso di mancata attribuzione a uno Stato, infine, sussisterebbero alcuni obblighi di monitoraggio e prevenzione a carico dello Stato da cui l'operazione ostile ha avuto origine, il quale dovrebbe vigilare affinché il proprio territorio non venga impiegato per condurre operazioni ostili integranti un illecito internazionale. V. UN GGE Report 2021, cit., p. 10 ss. Per un'analisi, si veda, *ex multis*, F. DELERUE, *Cyber operations*, cit., pp. 193-260; A. BONFANTI, *op. cit.*, p. 718 ss.

dello *jus ad bellum* nel cyberspazio. A tal riguardo, ci si è sovente interrogati sulla possibilità che operazioni informatiche particolarmente offensive o intrusive possano, di per sé, configurarsi come un uso illecito della forza.

Come noto, la CNU disciplina il ricorso alla forza armata tra Stati sotto tre profili: sotto il profilo del divieto dell'uso e della minaccia, laddove essa sia rivolta contro «l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite» (art. 2, par. 4) [48]; indentificando l'«atto di aggressione» quale condizione necessaria per l'esercizio da parte del Consiglio di Sicurezza dei poteri coercitivi ad esso attribuiti dal Capitolo VII della CNU (art. 39); o indicando l'«attacco armato» quale presupposto per l'esercizio, da parte dello Stato vittima dell'attacco, del proprio «diritto naturale» di legittima difesa, sia individualmente che collettivamente [49].

Il divieto di ricorrere alla forza armata corrisponde non solo a un obbligo autonomo di carattere generale [50], ma – in virtù della fondamentale importanza che esso riveste nella configurazione contemporanea dell'ordinamento internazionale – ha assunto altresì l'efficacia di norma cogente o imperativa [51], traducendosi, nel rapporto tra le fonti, in termini di inderogabilità, di fatto implicando la nullità di qualsiasi trattato che abbia a oggetto un impiego vietato della forza armata [52].

L'estensione della disciplina in esame al contesto del cyberspazio è un compito tutt'altro che semplice, giacché la Carta non contiene alcuna definizione delle nozioni di «forza» o «attacco armato» che consenta di circoscrivere l'ambito di applicazione delle disposizioni convenzionali rilevanti a determinate

---

[48] Per ragioni di spazio, il presente scritto si concentra esclusivamente sulla possibile qualificazione di condotte cibernetiche alla stregua di uso illecito di forza, senza approfondire il tema del divieto della minaccia di tale uso. Per un'analisi sulla minaccia dell'uso della forza in ambito *cyber*, si veda: M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., pp. 338-339; J. SKINGSLEY, *'Cyber-rattling: can 'pre-positioning' in cyberspace amount to a threat of the use of force under Article 2(4) of the United Nations Charter?*, in *Journal on the Use of Force and International Law*, 2024, vol. 11, n. 1-2, pp. 50-86.

[49] M. ARCARI, *La crisi in Crimea*, in *Diritti umani e diritto internazionale*, 2014, vol. 8, n. 2, pp. 474-477.

[50] Caso *Nicaragua*, cit., par. 173; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004*, par. 87.

[51] *Commentary of the Commission to Article 50 of its draft Articles on the Law of Treaties, ILC Yearbook, 1966-11*, p. 247, par. 1; Caso *Nicaragua*, cit., par. 190. Si vedano, inoltre, le posizioni sul diritto internazionale applicabile al cyberspazio di: Unione Africana; Austria, Brasile, Cuba, Repubblica ceca.

[52] Convenzione di Vienna sul diritto dei trattati del 23 maggio 1969, in *UNTS*, vol. 1155, 332, art. 53; M. ARCARI, *Uso della forza [dir. int.]*, in Diritto online [2014], in www.treccani.it; A. CASSESE-M. FRULLI (a cura di), *op. cit.*, p. 305 ss.

condotte statali, siano esse *cyber* o meno. Né esiste, del resto, una disciplina convenzionale *ad hoc* applicabile alle attività degli Stati mediante ICT tale da chiarire le condizioni entro cui specifiche operazioni informatiche possano considerarsi alla stregua di un ricorso illecito alla forza o un attacco armato.

Tale classificazione non assolve uno scopo puramente formale, in quanto la qualificazione di talune operazioni come attacco armato *ex* art. 51 CNU consentirebbe allo Stato vittima di reagire in legittima difesa, sia tramite mezzi *cyber* che convenzionali. Sul piano della responsabilità internazionale dello Stato, poi, dalla natura cogente del divieto di ricorrere all'uso della forza discende, in caso di violazione grave, una serie di obblighi aggiuntivi a carico di tutti gli Stati. Questi si sostanziano nel divieto di riconoscere come legittima la situazione creatasi per effetto di tale violazione, di fornire assistenza o aiuto all'autore nel mantenerla in essere, e nell'obbligo di cooperare per porvi fine [53].

Quanto al contenuto del divieto di cui all'art. 2, par. 4, esso è ritenuto applicabile al solo ricorso alla forza *armata* tra Stati [54], di fatto escludendo dalla nozione la mera coercizione economica o politica [55]. Sul punto, la CIG ha chiarito che – benché il divieto di utilizzare la forza non si riferisca a specifiche armi, ma si estenda «*to any use of force, regardless of the weapons employed* [56]» – non tutte le forme di intervento illecito infrangono il divieto *de quo*, stabilendo nel caso *Nicaragua* che il "mero" finanziamento di movimenti ribelli non costituisca un uso illecito della forza, quanto piuttosto una forma di coercizione politica. Diversamente, uno Stato che addestri e fornisca armi a gruppi armati

---

[53] Cfr. artt. 26, 40, 41 e 48 del *Draft Articles on Responsibility of States*, cit.; M. ARCARI, *La crisi in Crimea*, cit., p. 477.

[54] C. TAMS, *Article 2 (4)*, in B. SIMMA-D.E. KHAN-G. NOLTE-A. PAULUS (eds.), *The Charter of the United Nations: A Commentary*, IV ed., Oxford University Press, Oxford, 2023, p. 310 ss. Tale disposizione, applicandosi «nelle relazioni internazionali», ossia nei rapporti tra Stati, non preclude tuttavia a uno Stato la possibilità di utilizzare la forza o la minaccia della stessa nei confronti di attori non statali presenti sul proprio territorio, quali insorti o agenti diplomatici stranieri. Cfr. C. FOCARELLI, *Trattato di diritto internazionale*, UTET Giuridica, Milano, 2015, p. 1770.

[55] Tale conclusione può essere dedotta dal preambolo della CNU («*armed force shall not be used, save in common interest*»), nonché dai lavori preparatori. Si veda, I. BROWNLIE, *International Law and the Use of Force by States*, Oxford University Press, Oxford, 1963, p. 362; M.N. SCHMITT, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, p. 907 ss.; D. SILVER, *Computer Network Attack as a Use of Force under Article 2(4)*, in M. SCHMITT-B. O'DONNELL (eds), *Computer network attack and international law*, Naval War College, Newport, 2002, pp. 80-82 («*… no international consensus has emerged defining economic and political coercion, standing alone, as force*»). Si veda, inoltre, la posizione dei Paesi Bassi.

[56] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996,* par. 39.

organizzati per condurre operazioni militari contro un altro Stato violerebbe l'art. 2, par. 4, purché il conseguente attacco superi la soglia implicante l'uso della forza armata [57]. Ciò varrebbe anche nell'ipotesi in cui l'arma fornita sia un *malware* necessario per condurre un'operazione informatica ostile che provochi una certa soglia di danno, come avremo modo di approfondire [58]. Difatti, in virtù delle enormi potenzialità distruttive di taluni *software* malevoli, autorevole dottrina ha affermato che «*cyber … must be looked upon as a new means of warfare-in other words, a weapon: no less and no more than other weapons*» [59].

5. Dalla «forza cibernetica» agli attacchi informatici: le soglie dello *jus contra bellum* nell'era digitale

Escluse dall'ambito di analisi le forme di intervento coercitivo di tipo politico o economico, persiste la questione, «piuttosto controversa [60]», di determinare le soglie necessarie affinché un'operazione informatica sponsorizzata da uno Stato possa raggiungere il livello dell'uso della forza armata e configurare una possibile violazione dell'art. 2, par. 4. A tale riguardo, tre sono gli approcci elaborati in dottrina volti a indagare tale ipotesi: *instrument-based* (basato sui mezzi utilizzati), *target-based* (basato sull'obiettivo), ed *effects-based* (basato sulle conseguenze) [61].

Il primo approccio è stato soggetto a critiche, poiché – concentrandosi esclusivamente sulle caratteristiche fisiche dell'arma impiegata per sferrare l'attacco – escluderebbe la possibilità che capacità cibernetiche possano, da sole, integrare la soglia della forza armata a prescindere dalle conseguenze, anche gravi,

---

[57] Caso *Nicaragua*, cit., par. 228; M.C. VITUCCI, *Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo-ucraino*, in *La Comunità Internazionale*, 2023, vol. 1, p. 17. L'A. suggerisce che tale ipotesi potrebbe trovare riscontro nella fornitura di *software* e relativo addestramento delle milizie siriane antigovernative da parte degli Stati Uniti.

[58] M.N. SCHMITT, *Tallinn Manual 2.0*, cit., p. 332. V. *infra* par. 5.

[59] Y. DINSTEIN, *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*, in *International Law Studies*, 2013, vol. 89. Sulla possibilità di classificare un *malware* come arma ai sensi dell'art. 2, par. 4, si veda M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, pp. 302-303.

[60] M. ROSCINI, *Cyber operations as a use of force*, in N. TSAGOURIAS-R. BUCHAN, *op. cit.*, p. 229; F. DELERUE, *Cyber Operations*, cit., p. 284.

[61] O. HATHAWAY-R. CROOTOF-P. LEVITZ-H. NIX-A. NOWLAN-W. PURDUE-J. SPIEGEL, *The Law of Cyber-Attack*, in *California Law Review*, vol. 100, n. 4, 2012, p. 845 ss.

che talune operazioni informatiche ostili potrebbero produrre, specialmente laddove siano dirette contro infrastrutture vitali per la popolazione, come l'acqua, l'energia o la sanità [62]. Similmente, l'approccio fondato sull'obiettivo dell'attacco informatico, secondo cui *qualsiasi* operazione che penetri nell'infrastruttura critica nazionale, indipendentemente dai danni generati, sia da considerarsi alla stregua di un attacco armato [63] non risulta del tutto convincente, anche alla luce dell'assenza di una definizione condivisa di tali infrastrutture. Tale orientamento, inoltre, non terrebbe conto della pluralità di conseguenze che un attacco informatico potrebbe produrre, poiché ricondurrebbe alla nozione di uso della forza armata, incluse le sue forme più gravi di attacco armato [64], anche operazioni che provochino effetti temporanei non particolarmente gravi, purché diretti contro settori che lo Stato individua come critici [65].

Accanto ad alcune autorevoli e condivisibili voci a favore dell'adozione di criteri combinati [66], vi è un consenso crescente volto a subordinare la qualificazione di un'operazione informatica quale uso illecito della forza armata alle conseguenze che essa produce. Secondo l'approccio basato sull'equivalenza cinetica, il c.d. *effects-based approach*, invero, un'operazione informatica potrebbe integrare la soglia di forza di cui all'art. 2, par. 4, laddove i suoi effetti risultassero equiparabili a quelli prodotti da un attacco cinetico, ossia sferrati tramite un'arma "tradizionale" [67]. In altre parole, rientrerebbero nella nozione tutte quelle operazioni mediante ICT che, attraverso l'alterazione, la cancellazione o il danneggiamento di software o dati, siano suscettibili di provocare, sia direttamente che indirettamente, danni fisici a beni o proprietà, nonché lesioni a persone o la perdita di vite umane, in misura comparabile ad attacchi fisici [68].

---

[62] S.P. KANUCK, *Information Warfare: New Challenges for Public International Law*, in *Harvard International Law Journal*, vol. 37, n. 1, 1996, p. 288-289. *Contra*, si vedano: D.B. HOLLIS, *Why States Need an International Law for Information Operations*, in Lewis & Clark Law Review, vol. 11, n. 4, 2007, p. 1040 ss.; R. NGUYEN, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, in *California Law Review*, vol. 101, n. 4, 2013, p. 1117.

[63] W. SHARP, *CyberSpace and the Use of Force*, Aegis Research Corporation, 1999, pp. 129-131.

[64] Caso *Nicaragua*, cit., par. 191.

[65] Si vedano, sul punto, M.J. SKLEROV, *Solving the Dilemma of Sate Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent*, in *Military Law Review*, vol. 201, pp. 55-56; R. NGUYEN, *op. cit.*, p. 1119 ss.

[66] M. ROSCINI, *Cyber operations as a use of force*, cit., p. 302; F. *Delerue*, *Cyber operations*, cit., p. 290.

[67] M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 331.

[68] M. ROSCINI, *Cyber operations as a use of force*, cit., pp. 305-306; M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 330 ss. Si vedano, inoltre, le posizioni di: Unione Africana, Australia, Germania, Francia, Paesi Bassi, Svezia, Regno Unito, Stati Uniti.

Similmente, *cyber* operazioni con conseguenze particolarmente violente o distruttive, che causino gravi lesioni o la morte di un certo numero di persone, o che provochino danni significativi o la distruzione di proprietà, specialmente se sferrate in combinazione con attacchi tradizionali [69], e i cui effetti siano equiparabili a quelli ottenuti tramite armi convenzionali, potrebbero configurarsi alla stregua di un attacco armato di cui all'art. 51 [70], consentendo eventualmente allo Stato vittima dell'attacco di rispondere tramite la forza armata (sia tramite mezzi informatici che tradizionali), purché in modo conforme ai principi di proporzionalità e necessità [71].

Benché l'approccio dell'equivalenza cinetica non rifletta posizioni dottrinali pienamente unitarie [72], la quasi totalità degli Stati che finora hanno reso pubblica la propria posizione ufficiale sul diritto internazionale e il cyberspazio – sia individualmente che congiuntamente, per mezzo di organizzazioni internazionali – hanno descritto la soglia richiesta dall'art. 2, par. 4, in base alle conseguenze, ovvero alla portata e agli effetti («*scale and effects* [73]») dell'operazione informatica [74]. L'Italia, per esempio, considererebbe una specifica operazione informatica un uso illecito della forza armata «*when its scale and effects are comparable to those of a conventional use of force, resulting in physical damage of property, human injury or loss of life*». Altri Stati, pur considerando che ciascuna valutazione richieda un'analisi circostanziale [75], sembrano

---

[69] Si veda, ad esempio, la posizione ufficiale della Francia: «*Cyberattacks which do not reach the threshold of an armed attack when taken in isolation could be categorised as such if the accumulation of their effects reaches a sufficient threshold of gravity, or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or from different entities acting in concert*».

[70] Y. DINSTEIN, *Computer Network Attacks and Self-Defence*, in M. SCHMITT-B. O'DONNELL, *op. cit.*, p. 103.

[71] F. MARRELLA, *Diritto internazionale*, Giuffrè-Francis Lefebvre, Milano, 2023, pp. 741-742.

[72] Si vedano, ad esempio, le posizioni critiche nei confronti di orientamenti tesi a voler includere nella nozione di forza anche attacchi contro mercati finanziari o sistemi bancari. Sul punto, D. SILVER, cit., pp. 86-88; A. BUFALINI, *op. cit.*, pp. 418-419.

[73] Il criterio della portata e degli effetti, inizialmente impiegato dalla CIG per descrivere i criteri applicabili alla nozione di attacco armato, è stato successivamente ripreso dalla dottrina anche nell'ambito dell'art. 2, par. 4. M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 330 ss.

[74] M.N. SCHMITT-A. PAKKAM, *Cyberspace and the Jus ad Bellum: The State of Play*, in *International Law Studies*, 2024, vol. 103, p. 200 ss. Due posizioni contrarie in questo senso sono state avanzate da Cuba (2024), la quale ritiene «pericolosa» qualsiasi espansione «ingiustificata» delle nozioni di forza e attacco armato, e dalla Colombia (2025), la quale si limita a constatare che «*several questions on this issue remain open and need to be further addressed by States, particularly those related to the threshold of what constitutes force in cyberspace*».

[75] Si vedano le posizioni di Canada, Costa Rica, Finlandia, Germania, Italia.

avvalorare tale approccio, sottolineando come «*the effects of the operation determine whether the prohibition applies, not the manner in which those effects are achieved* [76]» o, ancora, che «*emphasis needs to put on the effects rather than the means used* [77]».

Alla luce di quanto sopra, è lecito domandarsi se, ai fini di una possibile configurazione di una violazione dell'art. 2, par. 4 tramite mezzi informatici, debba sussistere una soglia minima di gravità delle conseguenze prodotte da determinate operazioni, in termini di distruzione di beni o ferimento di persone, oppure se, in assenza di tale requisito, queste debbano piuttosto considerarsi contrarie ad altre norme di diritto internazionale. Come noto, infatti, la nozione di operazione informatica comprende una pletora di attività di portata e dimensione variabili, suscettibili di provocare conseguenze disparate, dall'alterazione o distruzione di dati, al sabotaggio di strutture, al ferimento o alla morte di persone [78]. Benché tale questione appaia ancora dibattuta, e tenuto conto dell'esistenza di alcune posizioni dottrinali a favore della sussistenza di un livello di violenza minima prodotta dall'attacco [79], l'art. 2, par. 4, come autorevolmente asserito da Ago, vieta «*any kind of conduct involving any assault whatsoever on the territorial sovereignty of another State, irrespective of its magnitude, duration or purposes*» [80]. Ne consegue che qualsiasi qualificazione di condotte *cyber* attribuite a uno Stato come uso della forza presupporrebbe necessariamente una valutazione delle circostanze del caso: tanto più intrusiva e distruttiva l'azione, tanto maggiore sarebbe la propensione dello Stato (o degli Stati) vittima a qualificarla come una violazione dell'art. 2, par. 4 [81].

Secondo tale impostazione, sembrerebbe che operazioni di tipo DoS o DDoS, ovvero tese a impedire l'accesso a determinati servizi senza particolari effetti sul piano materiale – ad esempio, l'interruzione temporanea di un sito *web* di una Università pubblica [82] – o le cosiddette operazioni di tipo psicologico finalizzate a minare la fiducia dei cittadini nei confronti di un dato governo o influenzare l'opinione pubblica [83] – difficilmente possano produrre

---

[76] V. la posizione della Germania.

[77] V. la posizione dei Paesi Bassi.

[78] F. DELERUE, *Cyber operations*, cit., p. 294.

[79] M.N. SCHMITT (eds), *Tallinn Manual 2.0*, p. 334.

[80] R. AGO, *Addendum to the Eight Report on State Responsibility*, in *Yearbook of the ILC II/1*, 1980, p. 44. Si veda, inoltre, N. MELZER, *Cyberwarfare and international law*, United Nations Institute for Disarmament Research (UNIDIR) Resources, 2011, p. 8.

[81] M. ROSCINI, *Cyber operations as a use of force*, cit., p. 308.

[82] *Ibidem*.

[83] M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 331. Un esempio in questo senso ci è fornito dalle operazioni di influenza israeliane denominate *hasbara*, ossia forme di *public diplomacy* volte

conseguenze tali da configurarsi come forza armata e integrare una violazione dell'art. 2, par. 4, né tantomeno come attacco armato *ex* art. 51, ancorché non necessariamente conformi ad altri obblighi di natura internazionale. Tali operazioni, infatti, potrebbero violare altre norme di diritto internazionale, quali il principio di non intervento negli affari esterni o interni di un altro Stato e/o il principio di sovranità [84].

6. *Cyber* "attacchi" contro infrastrutture critiche: un'evoluzione della dottrina dello *jus ad bellum*?

In linea di principio, secondo l'approccio basato sull'equivalenza cinetica brevemente delineato poc'anzi, il fatto che un'operazione informatica abbia come bersaglio un'infrastruttura critica non è, di per sé, determinante nella qualificazione di tale operazione come un uso illecito della forza [85]. Tuttavia, alcuni autori hanno opportunamente osservato che la dipendenza pressoché totale delle nostre società dai mezzi di informazione e comunicazione, inclusi i computer, le reti e i sistemi informatici, consentirebbe di ottenere esiti analoghi e altrettanto dannosi rispetto agli attacchi tradizionali, senza necessariamente implicare la distruzione di tali reti o sistemi [86]. È piuttosto evidente, infatti, che l'interconnessione delle reti, congiuntamente alla crescente sofisticazione delle capacità informatiche (sia statali, che non), permettano di ottenere conseguenze particolarmente gravi tramite la "semplice" disabilitazione di reti e sistemi su cui infrastrutture critiche operano: si consideri il caso di un attacco informatico alla centrale idroelettrica che causi *blackout* su vasta scala, e che renda inoperativi ospedali o servizi pubblici, o l'interruzione prolungata di sistemi finanziari con significativi effetti transfrontalieri [87].

Tali ipotesi hanno indotto alcuni autori a considerare l'approccio fondato sull'equivalenza cinetica eccessivamente «restrittivo [88]» e a valutare un «riorientamento interpretativo [89]» dell'art. 2, par. 4, volto a considerare forza armata

---

a influenzare la narrazione che riguarda Israele. Sul punto, si veda R. ALLEGRI-G. SCICHILONE, *op. cit.*, p. 9 ss.

[84] R. BUCHAN, *op. cit.*, pp. 211-228; P. ROGUSKI, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program For Cyber Norms Policy Brief, 2020, p. 4 ss.

[85] M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., p. 328.

[86] M. ROSCINI, *Cyber operations and the Use of Force in International Law*, cit., p. 48 ss.

[87] M. ROSCINI, *Cyber operations as a Use of force*, cit., p. 310.

[88] N. MELZER, *op. cit.*, p. 14.

[89] M.C. WAXMAN, *op. cit.*, p. 437.

– o attacco armato *ex* art. 51 – anche *cyber* operazioni che causino una perdita grave della funzionalità di infrastrutture critiche o producano considerevoli effetti perturbatori tali da paralizzare o compromettere gravemente il funzionamento dell'apparato statale [90], indipendentemente dalle conseguenze sul piano materiale.

Tali posizioni dottrinali hanno trovato qualche limitato riscontro, seppur in diversa misura, nelle posizioni ufficiali degli Stati. Sebbene alcuni mantengano una certa cautela in ordine alla qualificazione di operazioni non distruttive come uso della forza armata [91], altri Stati, come la Francia, i Paesi Bassi e la Norvegia, non escludono del tutto tale ipotesi, purché l'operazione in questione soddisfi alcuni criteri di tipo qualitativo e quantitativo [92]. Questi includono, ad esempio, la gravità delle conseguenze, le circostanze prevalenti al momento dell'operazione, l'origine dell'operazione e la natura dell'istigatore (militare o meno), l'entità dell'intrusione, gli effetti reali o previsti dell'operazione e la velocità con cui essi sono prodotti, e la natura del bersaglio dell'attacco [93]. Proprio rispetto a quest'ultimo criterio, non sorprende che diverse posizioni ufficiali ammettano la possibilità di considerare un uso illecito della forza armata operazioni che producano una perdita significativa della funzionalità di talune infrastrutture ritenute critiche o vitali – quali il sistema bancario o finanziario, le telecomunicazioni, la fornitura elettrica o le scorte di vaccini – indipendentemente dalla loro capacità distruttiva [94]. Un esempio in tale senso ci è offerto

---

[90] M. ROSCINI, *Cyber operations as a Use of force*, cit., p. 309; N. TSAGOURIAS, *Cyber attacks, self-defence and the problem of attribution*, in *Journal of Conflict and Security*, vol. 17, p. 231 (suggerendo che «*an attack on a State's financial system which, by modifying or corrupting data, causes massive disruption to the economic life of a State, should qualify as an armed attack*»).

[91] Si vedano, ad esempio, le posizioni dell'Italia, Israele, Finlandia.

[92] Tali criteri, inizialmente elaborati da Schmitt, sono stati adottati e ulteriormente precisati dagli Esperti del Manuale di Tallinn al fine di individuare quali operazioni «*short of an armed attack*» potrebbero violare l'art. 2, par. 4. Essi includono: *severity* (il grado di gravità, durata, e intensità delle conseguenze); *immediacy* (velocità con cui le conseguenze dell'attacco si manifestano); *directness* (il livello di causalità tra l'attacco in sé e le dirette conseguenze); *invasiveness* (il grado di intrusione all'interno dei sistemi dello Stato vittima); *measurability* (la facilità con cui è possibile valutare la misura delle conseguenze prodotte dall'attacco); *military character* (il carattere militare dell'operazione); *State involvement* (il grado di coinvolgimento statale); *presumptive legality* (la presunta legalità dell'azione). Va inoltre notato che gli Stati, nelle loro posizioni ufficiali, «*tend to pick and choose from among the* Tallinn Manual *factors when highlighting relevant factors, sometimes adding their own*». M.N. SCHMITT, *Computer Network Attack*, cit., p. 914; M.N. SCHMITT (eds), *Tallinn Manual 2.0*, cit., p. 333 ss.; M.N. SCHMITT-A. PAKKAM, *op. cit.*, p. 205 ss.

[93] V. le posizioni di Unione Africana, Francia, Paesi Bassi.

[94] V. posizioni di Costa Rica, Danimarca, Irlanda, Paesi Bassi, Norvegia. Altri Stati, come la Tailandia e l'Estonia richiedono un certo danno materiale a seguito del danneggiamento o della

dalla posizione dell'Italia, la quale, pur concedendo che la questione risulti ancora «controversa», non ha escluso che operazioni che causino l'interruzione di servizi essenziali per la popolazione senza danni fisici possano ricadere nell'ambito di applicazione dell'art. 2, par. 4.

Tali constatazioni inducono a domandarci se la prassi recente si sia evoluta nel senso di considerare operazioni informatiche non distruttive alla stregua di un uso proibito della forza ai sensi dell'art. 2, par. 4, laddove queste siano sferrate contro infrastrutture critiche e determinino effetti significativi sulla sicurezza e la stabilità dello Stato vittima. Per un verso, un'interpretazione evolutiva delle disposizioni della CNU è ammessa dall'art. 31 della Convenzione di Vienna sul diritto dei trattati del 1969, il quale prevede che – nell'interpretazione di un trattato – si debba tenere conto «di qualsiasi prassi successivamente seguita nell'applicazione del trattato» e, in aggiunta al contesto, «di qualsiasi regola pertinente di diritto internazionale applicabile nei rapporti tra le parti» [95]. Sarebbe, dunque, ipotizzabile – e, secondo alcuni, raccomandabile – conferire un significato evolutivo [96] alla nozione di forza *ex* art. 2, par. 4, tale da rispecchiare l'evoluzione degli armamenti e i nuovi impieghi della forza, anche tramite mezzi ICT [97]. Per altro verso, ci appare prematuro, allo stato attuale, presumere un'evoluzione della prassi in tal senso, in ragione di alcune considerazioni.

Come anticipato, l'assenza di una definizione univoca e condivisa di infrastruttura critica comporta un certo grado di incertezza riguardo a quali specifici settori sarebbero protetti da attacchi, e la cui individuazione, ricordiamo, è

---

perdita di funzionalità dell'infrastruttura critica oggetto dell'attacco. Va notato che, giacché gli effetti di operazioni mediante ICT tendono a manifestarsi in maniera indiretta, nel trattare la questione delle operazioni informatiche contro settori critici rileva – in aggiunta al criterio del *target* dell'attacco informatico – il criterio della *directness*, ossia il nesso di causalità tra l'operazione informatica e le conseguenze prodotte. Secondo tale criterio, quanto più gli effetti dannosi di un'operazione informatica siano ad essa riconducibili, tanto più lo Stato che ne subisce le conseguenze sarà propenso a classificarla come uso vietato della forza armata; al contrario, laddove il nesso tra atto iniziale ed effetti risulti attenuato, tale qualificazione risulterà meno probabile. V. M.N. SCHMITT (eds), *Tallinn Manual 2.0*, cit., p. 334.

[95] Convenzione di Vienna sul diritto dei trattati, 23 maggio 1969, art. 31, par. 3, lett. b) e c); A. CASSESE-M. FRULLI, *op. cit.*, p. 281.

[96] *Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2009*, par. 66 («*where the parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered into for a very long period or is "of continuing duration", the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning*»).

[97] A. SEGURA-SERRANO, *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, 2006, vol. 19, p. 225; M. ROSCINI, *Cyber operations as a use of force*, cit., pp. 309-310.

lasciata alla piena discrezionalità statale [98]. Si pensi all'infrastruttura elettorale, designata come critica dagli Stati Uniti nel 2017 solo a seguito delle interferenze russe nella precedente elezione [99]. Non solo: alcuni Stati si sono dichiarati restii a designare determinati settori come critici, per timore che ciò possa giustificare implicitamente attività ostili contro quelli non già espressamente individuati [100]. Peraltro, un numero ancora esiguo di Stati si è espresso in tal senso, mentre gran parte delle posizioni ufficiali continua a richiedere che l'operazione informatica determini un certo livello di danno materiale affinché possa configurarsi una violazione dell'art. 2, par. 4.

Al contempo, va indubbiamente notato un crescente sostegno, sia in dottrina che tra gli Stati che hanno reso pubbliche le proprie posizioni sul diritto internazionale applicabile al cyberspazio, a considerare talune operazioni informatiche non distruttive che provocano il malfunzionamento del sistema finanziario o il collasso di settori dell'economia, una destabilizzazione diffusa o ingenti ripercussioni economiche, alla stregua di uso della forza armata *ex* art. 2, par. 4 [101], e – nei casi particolarmente gravi – come un attacco armato *ex* art. 51 [102].

Alla luce di quanto sopra, ci sembra plausibile ritenere che il fatto che un'operazione ostile abbia come obiettivo un'infrastruttura critica, come la sanità pubblica, i trasporti o il sistema finanziario, possa costituire un elemento a favore della sua qualificazione come uso della forza, anche laddove non siano prodotte conseguenze sul piano materiale. Diversamente, qualora l'operazione in questione non producesse distruzione o non colpisse un'infrastruttura individuata come critica dallo Stato vittima, sarebbe inverosimile che questo possa invocare l'art. 2, par. 4 [103].

Neppure ci sembra convincente l'ipotesi che esista, allo stato attuale, un

---

[98] A. BUFALINI, *op. cit.*, p. 420 ss.

[99] S. HAATAJA, *op. cit.*, p. 427.

[100] *Ibid.*; J. WEAVER, *Submission of Australia's independent expert to the United Nations Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (GGE)*, 20 maggio 2020, p. 8, in www.dfat.gov.au.

[101] Cf. la posizione della Repubblica ceca; Danimarca; Paesi Bassi; Norvegia. Si vedano, sul punto, M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, cit., p. 59 ss.; M. SCHMITT-J. BILLER, *The NotPetya Cyber Operation as a Case Study of International Law*, 2017, in www.ejiltalk.org; J. SPÁČIL, *Cyber Operations against Critical Financial Infrastructure: a Non-Destructive Armed Attack?*, in *International and Comparative Law Review*, 2022, vol. 22(2), p. 35 ss.

[102] V. la posizione della Francia («*Une cyberattaque pourrait être qualifiée d'agression armée dès lors qu'elle provoquerait des pertes humaines substantielles, ou des dommages physiques ou économiques considérables*»); M.N. SCHMITT-A. PAKKAM, *op. cit.*, pp. 207-208.

[103] Sul punto, si veda F. DELERUE, *Cyber operations*, cit., p. 304.

obbligo autonomo che vieti agli Stati di condurre operazioni ostili contro infrastrutture critiche. Innanzitutto, le *cyber norms* sul comportamento responsabile degli Stati, e in particolare la norma 13(f) brevemente trattata in precedenza, non chiariscono l'origine di un presunto divieto di condurre operazioni informatiche contro infrastrutture critiche, nell'ipotesi in cui queste non infrangano norme di diritto internazionale. Sembra condivisibile, ad avviso di chi scrive, l'opinione secondo cui il quadro per il comportamento responsabile degli Stati nel cyberspazio elaborato in ambito ONU, nel richiamare gli obblighi già esistenti in capo agli Stati in materia, introduca un ulteriore grado di complessità nell'interpretazione di taluni obblighi e divieti, specialmente per quanto concerne quelle operazioni non distruttive che, per gravità e dimensioni, non costituirebbero, secondo l'approccio prevalente, un ricorso illecito alla forza armata [104].

Va, inoltre, notato che – malgrado la crescente preoccupazione rispetto alle vulnerabilità di settori critici o vitali – essi continuano a essere oggetto di attacchi informatici che ne implicano la distruzione o il danneggiamento [105]. Benché sia stato sottolineato come la frequenza di tali attività ostili non determini necessariamente l'insorgere di una norma permissiva di diritto internazionale, tali operazioni non sembrano essere state accompagnate da specifiche reazioni di condanna da parte degli Stati tali da suggerire l'emergere di una norma proibitiva autonoma che vieti operazioni informatiche contro infrastrutture critiche, eccettuato il caso in cui esse infrangano altre norme di diritto internazionale [106].

7. Considerazioni conclusive

La presente trattazione ha tentato di mettere in luce alcuni aspetti tuttora controversi della regolamentazione del cyberspazio. Per un verso, come richiamato in apertura, non sono mancati gli sforzi della comunità internazionale volti a

---

[104] S. HAATAJA, *op. cit.*, p. 439 ss.

[105] M. HATHAWAY, *When Violating the Agreement Becomes Customary Practice*, in F.O. HAMPSON-M. SULMEYER (eds), *Getting beyond Norms*, Centre for International Governance Innovation, Waterloo, 2017, p. 6 («*Disrupting or damaging critical infrastructures that provide services to the public has become customary practice – the new normal. In the past two years and since the GGE agreement, there have been an alarming number of harmful incidents targeting critical infrastructures around the world, ranging from power systems to telecommunications systems to transportation systems to financial systems*»).

[106] Caso *Nicaragua*, cit., par. 207; *North Sea Continental Shelf, Judgment, I.C.J. Reports 1969*, par. 77. Si veda, sul punto: https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_grid.

delineare linee guida condivise, con lo scopo di orientare il comportamento degli Stati nell'impiego responsabile delle tecnologie dell'informazione e della comunicazione. Per altro verso, le caratteristiche intrinseche del contesto digitale, unite alla nota reticenza degli Stati a chiarire pubblicamente le proprie posizioni in materia [107], fanno sì che persistano ampie aree grigie che meriterebbero ulteriori approfondimenti.

Tali incertezze emergono in modo particolarmente evidente con riguardo allo *jus ad bellum* e, in particolare, alla sua rilevanza e concreta applicabilità al dominio *cyber*. La difficoltà di attribuire con certezza condotte mediante ICT, aggravata dal ricorso sempre più frequente, da parte degli Stati, ad attori non statali [108], si accompagna a quella di stabilire con chiarezza a quali condizioni talune operazioni possano configurarsi come uso della forza armata. È proprio in relazione alle soglie di forza già discusse che si riscontra una certa tendenza, da parte di alcuni Stati, a (dichiarare di) voler considerare applicabile l'art. 2, par. 4, anche a operazioni informatiche non distruttive, qualora esse – colpendo infrastrutture critiche sul territorio dello Stato (o degli Stati) vittima – provochino effetti perturbatori significativi tali da rendere inoperativi servizi essenziali per lo Stato e la popolazione.

Stante l'assenza, allo stato attuale, di una disciplina convenzionale applicabile al cyberspazio che chiarisca le questioni più controverse, un simile orientamento terrebbe in debito conto la totale dipendenza delle nostre società dai sistemi e dalle reti informatiche. Esso avrebbe inoltre l'effetto di stigmatizzare tali operazioni, impendo, del resto, che possano essere impiegate come contromisure in risposta a illeciti internazionali [109].

D'altronde, come riconosciuto dagli Esperti del Manuale di Tallinn, al netto del continuo emergere ed evolversi delle minacce nel cyberspazio, non è escluso che la prassi degli Stati possa anch'essa evolversi e contribuire a una progressiva reinterpretazione dello *jus ad bellum* [110].

---

[107] M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, cit., («*because State cyber practice is mostly classified and publicly available expressions of* opinio juris *are sparse, it is difficult to definitively identify any cyberspecific customary international law*»).

[108] A. STIANO, *op. cit.*, p. 262 ss.

[109] M. ROSCINI, *Cyber operations as a use of force*, cit., p. 313.

[110] M.N. SCHMITT (ed.), *Tallinn Manual 2.0*, p. 329.

Capitolo 5

Il dominio cyber negli attuali scenari di guerra mediterranei: il caso del conflitto in Medio Oriente

Riccardo Allegri [*], Giorgio Scichilone [**]

Abstract: Il 7 ottobre 2023 è cominciato un drammatico conflitto che ha visto coinvolti numerosi paesi mediorientali tra i quali: Israele, Palestina, Iran e Libano. Le operazioni militari tradizionali sono state accompagnate da azioni offensive e difensive afferenti al dominio cibernetico da parte di tutti gli attori coinvolti. La regione ospita infatti alcuni paesi tecnologicamente avanzati (Stato Ebraico e Repubblica Islamica) che possiedono dunque un notevole potenziale ma che al contempo prestano il fianco agli attacchi dei rivali. Inoltre, per la loro natura asimmetrica, le operazioni inerenti alla sfera digitale consentono anche ad attori diversi dagli stati, come Hamas e Hezbollah, di condurre azioni offensive contro Tel Aviv. Questo art. analizza le capacità cibernetiche dei belligeranti e, senza la pretesa di fornire un resoconto completo, intende mostrare come tali capacità siano state sfruttate nel corso del conflitto che ha sconvolto il Medio Oriente.

Keywords: Cyberwar – Cybersecurity – Israele – Hamas – Iran

---

[*] Assegnista di ricerca presso il Dipartimento di Scienze Politiche e delle Relazioni Internazionali dell'Università degli Studi di Palermo, riccardo.allegri@unipa.it. I parr. 1, 2 e 3 sono da attribuire a Riccardo Allegri. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

[**] Professore Ordinario di Storia delle Istituzioni Politiche presso il Dipartimento di Scienze Politiche e delle Relazioni Internazionali dell'Università degli Studi di Palermo, giorgio.scichilone@unipa.it. I parr. 4, 5 e 6 sono da attribuire a Giorgio Scichilone. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

Il terribile attentato terroristico del 7 ottobre del 2023 può già essere considerato uno spartiacque per la storia recente di Israele e Palestina, così come per quella più generale dell'intera regione mediorientale. Quel giorno, un elevato numero di militanti di Hamas, organizzazione classificata come terroristica da Stati Uniti ed Unione Europea, riuscì a forzare il blocco imposto da Israele sulla Striscia di Gaza, da essi controllata politicamente sin dal 2007, ed a riversarsi entro i confini dello Stato Ebraico. I paramilitari palestinesi uccisero indiscriminatamente oltre 1.300 persone e ne rapirono altre 250. Si trattò della peggiore azione terroristica nella storia del paese, sorto con la fine del protettorato britannico nel maggio del 1948, e del più grande massacro di ebrei dai tempi dell'olocausto. L'attacco è considerato dal *Global Terrorism Database* come quello con il più alto tasso di mortalità in rapporto alla popolazione, visto che ha raggiunto una *ratio* equivalente ad una vittima ogni 10.000 persone [1]. Come ha affermato l'allora Presidente degli Stati Uniti, Joe Biden, dato il numero di abitanti di Israele, l'attacco era proporzionalmente pari a 15 volte quello dell'11 settembre [2].

Tale evento ha prevedibilmente scatenato la risposta di Tel Aviv, che non si è fatta attendere. Il governo israeliano guidato da Benjamin Netanyahu, espressione di una coalizione che vede rappresentate anche le fasce più estreme della destra conservatrice del paese, ha dato avvio ad un conflitto ramificato su più fronti che dura ancora mentre si scrive. L'offensiva israeliana ha coinvolto la Striscia di Gaza, ove è in corso una grave crisi umanitaria, il Libano, l'Iran, la Sira e, in misura minore, lo Yemen, con importanti ripercussioni su tutto il Levante. Diverse potenze occidentali hanno contribuito allo sforzo bellico tramite la fornitura di armamenti, senza partecipare attivamente alle operazioni militari. Altre, come gli Stati Uniti, sono state coinvolte direttamente nel conflitto, avendo preso parte ai bombardamenti delle infrastrutture nucleari iraniane nel giugno del 2025 ed anche delle posizioni dei ribelli Houthi nel martoriato Yemen qualche mese prima [3]. Altre ancora, come la Francia, hanno provveduto a

---

[1] G. Baram-I. Ben Israel, *Redefining vigilance: reevaluating the meaning of early warning in Israel's security doctrine and the October 7 attack*, in *Intelligence and National Security*, 2025, vol. 40, n. 3, pp. 470-485.

[2] The White House, *Remarks by President Biden on the October 7th Terrorist Attacks and the Resilience of the State of Israel and its People*, https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2023/10/18/remarks-by-president-biden-on-the-october-7th-terrorist-attacks-and-the-resilience-of-the-state-of-israel-and-its-people-tel-aviv-israel/, 18 ottobre 2023.

[3] R. Michaelson, *'Nothing left to bomb': Yemen's civilians bear brunt of US airstrikes on Houthis*, in *The Guardian*, https://www.theguardian.com/global-development/2025/may/26/yemen-us-israeli-airstrikes-houthi-famine-humanitarian-crisis-civilians, 26 maggio 2025.

garantire il proprio contributo nella difesa dello Stato Ebraico dagli attacchi missilistici e dai droni iraniani, pur senza partecipare ad alcuna operazione offensiva [4].

Sebbene non sia possibile stabilire con certezza il numero di vittime provocato dalla rappresaglia israeliana, i portavoce di Hamas sostenevano, nel giugno del 2025, che nella sola Striscia di Gaza il conto dei morti avesse raggiunto le 55.000 unità [5]. Ma le stime variano moltissimo, al punto che in base al primo sondaggio indipendente condotto sul territorio, il numero delle vittime palestinesi per il periodo compreso tra l'ottobre del 2023 e il gennaio del 2025 era pari a 84.000 [6]. Secondo le Nazioni Unite, la maggior parte di esse – circa il 70% – era rappresentato da donne e bambini [7]. La catastrofe umanitaria è stata aggravata dal dramma dei milioni di sfollati, dalla quasi totale mancanza di beni di prima necessità e dallo spettro di un'incombente carestia che aleggia sulla Striscia di Gaza.

L'offensiva israeliana, che ha comportato un repentino allargamento del teatro di guerra ad altri paesi del Medio Oriente, ha determinato un mutamento nei rapporti di forza che caratterizzavano la regione nel suo complesso, almeno per quanto riguarda il breve periodo. L'Iran, percepito da Tel Aviv come minaccia esistenziale alla propria sicurezza e sospettato di aver preso parte alla pianificazione ed al finanziamento degli attentati del 7 ottobre, ha visto enormemente ridotto il proprio potenziale asimmetrico. Il profondo ridimensionamento dei suoi alleati, parte del cosiddetto "asse della resistenza" – Hamas, Hezbollah, Houthi e governo siriano di Assad – ha sensibilmente diminuito la minaccia posta da Teheran e la sua influenza sulla regione mediorientale appare decisamente in calo.

Ciò che ancora non è del tutto chiaro è se Israele sia riuscito a ristabilire un certo grado di deterrenza ed a garantirsi un futuro più sicuro con le proprie azioni.

Ad ogni modo, mentre il conflitto veniva combattuto lungo le dimensioni operative tradizionali – terra, mare ed aria – anche il dominio cibernetico assumeva

---

[4] J. IRISH, *France says it intercepted drones targeting Israel prior to Iran ceasefire*, in *Reuters*, https://www.reuters.com/world/middle-east/france-says-it-intercepted-drones-targeting-israel-prior-iran-ceasefire-2025-06-26/, 26 giugno 2025.

[5] W. SHURAFA-F. KHALED, *More than 55.000 Palestinians have been killed in the Israel-Hamas war, Gaza health officials said*, in *Associated Press*, https://www.ap.org/news-highlights/spotlights/2025/more-than-55000-palestinians-have-been-killed-in-the-israel-hamas-war-gaza-health-officials-say/, 11 giugno 2025.

[6] R. FIELDHOUSE, *First independent survey of deaths in Gaza reports more than 80.000 fatalities*, in *Nature*, 2025, vol. 643, pp. 311-312.

[7] M. MOENCH, *Nearly 70% of Gaza war dead verified by UN are women and children*, in *BBC News*, https://www.bbc.com/news/articles/cn5wel11pgdo, 8 novembre 2024.

una rilevanza non secondaria. Dopotutto, lo Stato Ebraico risulta una delle principali potenze mondiali in tale ambito, collocandosi appena al di sotto di USA, Cina e Federazione Russa. In effetti, a parte le notevolissime capacità offensive in possesso di Tel Aviv, Israele è stata spesso definita "*start-up nation*". Proprio in virtù di quanto si è appena affermato, la digitalizzazione che caratterizza il paese lo ha reso un obiettivo sotto questo profilo. Sebbene dotati di capacità nettamente inferiori rispetto a quelle del proprio avversario, l'Iran e i suoi *proxy* non si sono risparmiati nella guerra cibernetica contro lo Stato Ebraico. Senza contare che le particolari caratteristiche di questa tipologia di conflitto, che consente ai diversi attori di negare il proprio coinvolgimento in un'operazione, non determina quasi mai una risposta militare e ha un limitato potenziale di *escalation*, si prestano perfettamente al confronto asimmetrico tra i membri dell'"asse della resistenza" ed Israele. Non a caso, sebbene si sia registrato un notevole incremento degli attacchi *cyber* a partire dal 7 ottobre, il confronto in siffatto dominio era in corso già da diversi anni.

Nei paragrafi che seguiranno, si cercherà di comprendere il potenziale cibernetico dei principali attori coinvolti nel conflitto in Medio Oriente, partendo proprio da Israele per arrivare all'Iran, passando per Hamas e Hezbollah. Al contempo, si tenterà di descrivere la strategia sottesa all'impiego di tale strumento. Infine, si esaminerà il conflitto tutt'ora in corso nel quadrante levantino e mediorientale da un punto di vista strettamente cibernetico, evidenziando le principali operazioni.

2. Israele: strategia e potenziale della "start-up nation"

Come affermato in precedenza, Israele è noto come "*start-up nation*" in virtù del proprio vivace ecosistema tecnologico e perché possiede un elevato numero pro-capite di imprese attive nel settore ICT. Secondo l'indice pubblicato da *StartUpBlink*, riguardo la vitalità dell'ecosistema digitale lo Stato Ebraico si posiziona al terzo posto dietro USA e Regno Unito [8], mentre in base al *Global Innovation Index* esso è quindicesimo a livello globale (l'Italia, ad esempio, è ventiseiesima) [9]. In aggiunta, il *Global AI Index*, pubblicato da *Tortoise* e citato dallo stesso governo di Tel Aviv, classifica il paese come nono a livello mondiale e come secondo per investimenti pro-capite nel campo dell'intelligenza

[8] START UP BLINK, *Discover the Winners of the Innovation Economy*, https://www.startupblink.com/#rankings, 2025.

[9] WIPO, *Global Innovation Index 2024*, https://www.wipo.int/web-publications/global-innovation-index-2024/en/gii-2024-results.html, 2025.

artificiale [10]. Proprio per questi motivi, Israele risulta particolarmente esposto alle operazioni cibernetiche dei propri rivali. Non a caso, il governo di Tel Aviv fu tra i primi a riconoscere, oltre vent'anni fa, l'importanza strategica della cybersecurity per il proprio paese. D'altronde, esso risulta da tempo il principale bersaglio di attacchi e crimini informatici per quanto concerne la regione mediorientale. In base ai dati rilevati da *Microsoft Threat Intelligence*, nel report pubblicato nell'ottobre del 2023 (e dunque nel periodo antecedente l'inizio del conflitto), Israele figurava al primo posto tra i paesi dell'area MENA (*Middle East North Africa*) maggiormente colpiti in ambito cibernetico, avendo subito un quota pari al 38% di tutti gli attacchi informatici verificatisi in quel quadrante geografico [11]. Al contempo, però, e a corollario della sofisticatezza tecnologica che lo caratterizza, il paese possiede anche capacità offensive estremamente sviluppate.

A ben vedere, sia le esigenze nell'ambito della cybersecurity, sia il potenziale di attacco che Israele possiede, si innestano perfettamente nella cultura strategica del paese, che è prevalentemente, seppur aggressivamente, difensiva. Per quel poco che è dato sapere, vista la riservatezza degli apparati militari di Tel Aviv sulla questione – lo Stato Ebraico ed in particolare le *Israel Defense Forces* (IDF) hanno diffuso la loro prima dottrina sulla sicurezza nazionale soltanto nel 2015 – essi fondano la protezione del paese dalle numerose minacce incombenti sui seguenti assunti strategici: deterrenza, *early warning*, difesa, sconfitta del nemico e vittoria [12]. Chiaramente, per mantenere una postura di questo tipo, incentrata perentoriamente sul concetto di deterrenza come primo aspetto in grado di garantire la sopravvivenza di un paese che si percepisce – e per buona parte della sua storia effettivamente si è trovato – circondato da nemici ostili, lo sviluppo di un importante potenziale offensivo è determinante. E ciò vale anche in ambito cibernetico, ove peraltro, lo Stato Ebraico è stato, ed è tuttora, se possibile, ancor più riservato (almeno a livello militare) in tema di strategia. Ciononostante, Israele salì agli onori delle cronache già nel giugno del 2010, a seguito del danneggiamento delle centrifughe per l'arricchimento dell'uranio che si trovavano nell'impianto nucleare iraniano di Natanz e di diverse decine di migliaia di laptop. La causa di tale disastro fu un *worm* piuttosto sofisticato denominato *Stuxnet*, frutto di un progetto congiunto tra l'intelligence

[10] TORTOISE, *The Global AI Index*, https://www.tortoisemedia.com/data/global-ai#rankings, 2025.

[11] MICROSOFT THREAT INTELLIGENCE, *Microsoft Digital Defense Report, Building and improving cyber resilience*, 2023, p. 52.

[12] G. EIZENKOT, *Deterring Terror, How Israel Confronts the Next Generation of Threats*, traduzione inglese del documento strategico a cura del Belfer Center for Science and International Affairs della Harvard Kennedy School, 2016, pp. 11-12.

israeliana e quella statunitense e parte di un più ampio programma di attacchi cibernetici denominato "Operazione Giochi Olimpici" [13]. Dopotutto, nella stessa dottrina strategica del 2015 si faceva esplicito riferimento alla necessità di ricorrere alla guerra cibernetica per migliorare la deterrenza, in quelle che potrebbero essere definite azioni di *Computer Network Attack* (CNA). È poi interessante notare come, nel 2019, Israele abbia condotto un bombardamento mirato avente come bersaglio un intero edificio situato nella Striscia di Gaza. Al suo interno, secondo le IDF, lavoravano diversi hacker affiliati ad Hamas sospettati di condurre operazioni cibernetiche contro lo Stato Ebraico. Si è trattato quasi certamente della prima risposta militare convenzionale ad un attacco informatico [14].

Ma l'ambito *cyber* diviene ancor più fondamentale se si prende in considerazione il secondo principio strategico deputato a garantire la sopravvivenza dello Stato Ebraico, ovvero quello dell'*early warning*. Forse persino troppo, visto che tra le principali cause del fallimento dell'intelligence, reso evidente dalla totale incapacità di prevenire e poi di reagire tempestivamente agli attentati del 7 ottobre, vi sarebbe proprio un'eccessiva dipendenza dalla tecnologia, che si pensava fosse inaggirabile dal nemico e, magari, infallibile nelle sue capacità predittive [15]. Senza contare che, almeno rispetto ad Hamas, Israele possiede un enorme vantaggio competitivo dal momento che controlla direttamente l'intero sistema delle telecomunicazioni nella Striscia di Gaza, sia quelle *wired* che quelle *wireless*, compresa la rete internet [16]. Ad ogni buon conto, l'approccio cibernetico all'*early warning* è sottolineato anche all'interno del già citato documento strategico del 2015, laddove si identifica l'intelligence digitale come fondamentale per la raccolta di informazioni ed il monitoraggio degli avversari di Israele, in quelle che potrebbero essere definite operazioni di *Computer Network Exploitation* (CNE).

Infine, per ciò che concerne l'assunto della difesa pura e semplice come terzo pilastro atto a garantire la sopravvivenza dello Stato Ebraico, esso è ben rappresentato dalle due *National Cyber Security Strategy* pubblicate rispettivamente nel 2017 e nel 2025 dall'*Israel National Cyber Directorate* (INCD), ovvero l'organo responsabile, appunto, della difesa cibernetica, seppure nella sfera

---

[13] J. FARWELL-R. ROHOZINSKI, *Stuxnet and the Future of Cyberwar*, in *Survival, Global Politics and Strategy*, 2011, vol. 53, n. 1, pp. 23-40.

[14] F. CRISTIANO, *Palestine, Whose cybersecurity without cybersovregnty?*, in S. ROMANIUK-M. MANJIKIAN (eds), *Routledge Companion to Global Cyber-Security Strategy*, Routledge, Londra-New York, 2021, p. 422.

[15] C. JONES-R. GEIST PINFOLD, *Israel and the Politics of Intelligence Failure on 7 October*, in *The RUSI Journal*, 2025, vol. 170, n. 3, pp. 40-50.

[16] F. CRISTIANO, *Deterritorializing Cyber Security and Warfare in Palestine: Hackers, Sovereignty and the National Cyberspace as Normative*, in *CyberOrient*, 2019, vol. 13, n. 1, pp. 28-42.

civile. Ambedue i documenti adottano un approccio piuttosto simile che si basa essenzialmente su tre strati nel primo caso e su altrettanti pilastri nel secondo. La postura è decisamente difensiva in entrambi i testi, laddove i tre strati riguardano l'incremento della robustezza, quello della resilienza ed il miglioramento del potenziale di difesa dell'ecosistema digitale [17], mentre i tre pilastri fanno riferimento alla necessità di rendere sicuro lo spazio cibernetico nazionale partendo dal cittadino comune ed arrivando alle infrastrutture critiche, a quella di migliorare l'alfabetizzazione digitale della popolazione ed infine a quella di incrementare la cooperazione internazionale nell'ambito della cybersicurezza [18].

Un altro aspetto importante espresso nella dottrina militare pubblicata nel 2015 e che si colloca a metà tra le azioni offensive e quelle difensive e tra i domini cibernetico e cognitivo riguarda le operazioni di influenza delle percezioni e quelle di legittimazione [19]. A tal proposito diviene di assoluta rilevanza il concetto di *hasbara*, ovvero una particolare forma di *public diplomacy* intesa a persuadere i bersagli piuttosto che a influenzarne il comportamento tramite la manipolazione dell'informazione (del resto il termine significa proprio "spiegazione"). Se in passato essa aveva funzionato piuttosto bene, consentendo ad Israele di contrastare con buoni risultati le narrazioni rivali, almeno per quanto riguarda buona parte del mondo occidentale [20], durante l'attuale conflitto Tel Aviv sembra arrancare rispetto ai propri avversari, tanto che alcune voci si sono levate a suggerire di abbandonare un concetto di *hasbara* troppo autoreferenziale e poco orientato all'audience per passare invece a ben più assertive operazioni di influenza [21].

Dal punto di vista istituzionale, Israele ha modificato nel tempo la struttura delle agenzie che si occupano della cybersecurity. Fino al 2010, essa era prerogativa dello *Shin Bet*, ovvero l'apparato per l'intelligence interna, che a tal proposito aveva istituito un dipartimento apposito, l'unità nota come *National Information Security Agency* (NISA), attiva dal 2002. Essa aveva il compito di proteggere la rete internet, le infrastrutture critiche e quegli enti pubblici che erano considerati maggiormente a rischio [22]. Nel 2011, il governo di Tel Aviv

---

[17] ISRAEL NATIONAL CYBER DIRECTORATE, *Israel National Cyber Security Strategy*, in *Brief*, settembre 2017.

[18] ISRAEL NATIONAL CYBER DIRECTORATE, *Israel National Cyber Security Strategy*, 2025.

[19] G. EIZENKOT, *op. cit*., p. 38.

[20] M. AOURAGH, *Hasbara 2.0: Israel's Public Diplomacy in the Digital Age*, in *Middle East Critique*, 2016, vol. 25, n. 3, pp. 271-297.

[21] O. FRIDMAN-V. MICHLIN-SHAPIR-D. SIMAN-TOV, *From Hasbara (Public Diplomacy) to Influence in the Gaza War*, INSS Insight, King's College London, https://kclpure.kcl.ac.uk/portal/en/publications/from-hasbara-public-diplomacy-to-influence-in-the-gaza-war, 2023.

[22] F. CRISTIANO, *Israel, Cyber defense and security as national trademarks of international legitimacy*, in S. ROMANIUK-M. MANJIKIAN (eds), *op. cit*., p. 410.

dette mandato ad un gruppo di esperti di analizzare le vulnerabilità nell'impianto di sicurezza cibernetica esistente e proporre raccomandazioni utili a migliorare l'intero sistema, in quella che divenne nota come *National Cyber Initiative* (NCI). Seguendo i suggerimenti forniti dagli esperti, l'Ufficio del Primo Ministro istituì quindi quello che divenne noto come *National Cyber Bureau* (NCB), che a propria volta raccomandò alle autorità di creare un organismo espressamente dedicato alla sicurezza cibernetica in ambito civile. Nel 2017 nacque dunque quella che prese il nome di *National Cyber Security Authority* (NCSA). Infine, nel 2018 il governo israeliano decise di ristrutturare nuovamente il proprio ecosistema di sicurezza informatica ed accorpò l'NCSA e l'NCB, andando a formare l'attuale *Israeli National Cyber Directorate* (INCD) [23].

Se le istituzioni appena nominate hanno la responsabilità della difesa cibernetica civile, sono invece quelle delle IDF che si occupano delle operazioni offensive e di quelle di intelligence (oltre che, ovviamente, della protezione delle reti, delle infrastrutture e delle informazioni di natura militare). Le notevolissime capacità di Israele in questo ambito sono riconosciute a livello internazionale e sono il frutto dell'ambiente ostile nel quale il paese si trova incastonato. Per quanto concerne la salvaguardia delle reti e delle comunicazioni, esse sono di responsabilità dell'unità denominata *C4I and Cyber Defense Directorate* [24]. Per ciò che invece riguarda le operazioni offensive e quelle legate alla raccolta di informazioni, esse sono responsabilità della celebre unità 8200, inquadrata nell'*Aman*, ovvero l'intelligence militare. Tale organo delle forze armate, fondato nel 1952, si è tradizionalmente occupato di SIGINT (*signal intelligence*) e rappresenta l'equivalente israeliano della statunitense *National Security Agency* (NSA). Oltre alle operazioni di intercettazione e monitoraggio delle comunicazioni nemiche (ed al controllo delle attività informatiche della popolazione palestinese), l'unità 8200 è estremamente attiva anche in ambito offensivo. Si ritiene che essa possa celarsi dietro l'"Operazione Giochi Olimpici" e la diffusione di *Stuxnet* [25].

La raccolta di informazioni e le operazioni di intelligence in senso lato non sono prerogativa esclusiva dell'*Aman*. In tale ambito Israele si affida anche ad altre due organizzazioni, ovvero il già citato *Shin Bet* ed il famoso *Mossad*. Entrambe le agenzie fanno un uso estensivo delle moderne tecnologie informatiche e delle possibilità che il dominio cibernetico garantisce nel campo dell'intelligence. Del resto, gli apparati di sicurezza israeliani mantengono un rapporto

---

[23] J. Frei, *Israel's National Cybersecurity and Cyberdefense Posture, Policy and Organizations*, Cyberdefense Reports, Center for Security Studies, Zurigo, 2020, p. 5.

[24] IDF, *C4I and Cyber Defense Dorectorate*, https://www.idf.il/en/mini-sites/directorates/c4i-and-cyber-defense-directorate/c4i-and-cyber-defense-directorate/, 2021.

[25] S. Collins-S. McCombie, *Stuxnet: the emergence of a new cyber weapons and its implications*, in *Journal of Policing, Intelligence and Counter Terrorism*, 2012, vol. 7, n. 1, p. 87.

quasi incestuoso con il mondo delle *start-up* digitali, provvedendo al finanziamento di quelle ritenute maggiormente promettenti [26].

3. Hamas e Hezbollah: paramilitari nel dominio cibernetico

Le formazioni paramilitari che combattono lo Stato Ebraico e ne contestano l'esistenza non possiedono capacità cibernetiche che siano minimamente paragonabili a quelle israeliane. Eppure, la natura di questo particolare dominio consente ad attori come Hamas e Hezbollah di condurre operazioni informatiche efficaci anche in un contesto fortemente asimmetrico, seppur con un livello di sofisticatezza e con risorse economiche decisamente inferiori rispetto a quelle di Israele. Il quale, essendo un paese fortemente digitalizzato, presta il fianco ad attacchi nella sfera cibernetica.

Per quanto concerne Hamas, ovvero l'organizzazione che controlla la Striscia di Gaza dal 2007 e che è responsabile degli attentati del 7 ottobre, essa parrebbe aver investito parecchie risorse per sviluppare le proprie capacità informatiche, coerentemente con l'approccio multidimensionale e non-convenzionale tipico della formazione paramilitare. È necessario sottolineare come il ricorso all'impiego di strumenti cibernetici è perfettamente coerente con la strategia generale apparentemente adottata da Hamas nel corso degli anni e non rappresenta invece un cambiamento significativo del *modus operandi* dell'organizzazione. Nel dettaglio, la formazione paramilitare si pone da un lato l'obiettivo di porre termine all'esistenza di Israele e dall'altro quello di instaurare un regime islamico a guida palestinese. Prevedibilmente, per raggiungere tali risultati Hamas conduce quella che si può definire "lotta armata" contro lo Stato Ebraico e tenta al contempo di ottenere sempre maggiori consensi nella Striscia di Gaza ed in Cisgiordania [27]. Secondo Simon Handler, la leadership dell'organizzazione, in maniera del tutto razionale, è perfettamente consapevole dell'impossibilità attuale di sconfiggere militarmente e definitivamente Israele ed è maggiormente concentrata sull'erosione della (ormai poca) credibilità dell'Autorità Palestinese (AP). Per questo motivo, Hamas adotta una retorica infiammata che si richiama all'Islam più radicale, tentando di delegittimare coloro che, con maggiore moderazione, propongono la strada del dialogo con Tel Aviv.

---

[26] Cfr. *ex multis* MINISTRY OF INTELLIGENCE, *The Shin Bet's New Start-Ups in Collaboration with the Ministry of Intelligence: "Zionism and Innovation"*, https://www.gov.il/en/pages/news-startup230723, 2023.

[27] S. HANDLER, *The Cyber Strategy and Operations of Hamas, Green Flags and Green Hats*, Atlantic Council, Cyber Statecraft Initiative, 2022, p. 7.

Inoltre, almeno fino al 7 ottobre, il gruppo aveva condotto attentati terroristici contro Israele non soltanto con l'intento di destabilizzare il rivale, ma anche per guadagnare prestigio all'interno della comunità palestinese, a discapito dell'AP e per sabotare qualsiasi trattativa di pace con lo Stato Ebraico. In alcuni casi le ondate di attentati erano funzionali persino ad influenzare la politica israeliana in vista delle elezioni. Tali operazioni dovevano però mantenersi al di sotto di una certa soglia di violenza per evitare rappresaglie dannose per l'organizzazione. La possibilità di ricorrere al dominio cibernetico rappresenta evidentemente una perfetta soluzione per il perseguimento di siffatta strategia. Hamas può infatti condurre operazioni offensive contro Tel Aviv, anche a supporto di attentati terroristici, e proseguire nelle proprie azioni volte ad influenzare il popolo palestinese, quello israeliano e l'opinione pubblica a livello globale [28].

Fino al 7 ottobre, le attività di Hamas nella sfera cibernetica potevano essere suddivise in due categorie. Da un lato vi erano le operazioni di intelligence e raccolta di informazioni, mentre dall'altro vi erano quelle, appunto, di influenza. Per quanto riguarda le prime, esse parrebbero essere principalmente prerogativa delle cosiddette *Internal Security Forces* (ISF) ed in particolare dell'organismo noto come *Internal Security Agency* (ISA) [29]. In questo ambito, negli ultimi dieci anni si è registrato un evidente miglioramento qualitativo nelle azioni di Hamas. Nel 2013 prese avvio quella che fu ribattezzata *Operation Arid Vyper* che si articolava tramite una densa campagna di phishing. Essa prevedeva l'invio di e-mail contenti in allegato filmati pornografici che risultarono poi malevoli e che consentivano l'estrazione di informazioni dai dispositivi compromessi. I bersagli di tale operazione, non particolarmente sofisticata dal punto di vista dell'ingegneria sociale, furono diverse istituzioni governative israeliane, comprese le IDF [30]. Sebbene non sia possibile risalire con esattezza al colpevole, l'attacco parrebbe essere stato condotto dalla Striscia di Gaza e numerosi esperti lo attribuiscono ad Hamas. La campagna di phishing ottenne qualche successo ma non può essere considerata sofisticata e già nel 2015 si registrò un miglioramento tecnico non trascurabile, quando gli hacker dell'organizzazione terroristica presero ad includere dei link malevoli in sostituzione degli allegati tipici dell'operazione *Arid Vyper*, peraltro senza ricorrere soltanto alla pornografia. Nel 2017 poi essi incrementarono ulteriormente la complessità dell'operazione di esfiltrazione di dati sensibili creando dei falsi profili su Facebook e prendendo di mira specificamente il personale delle IDF tramite attività di ingegneria

[28] *Ivi*, pp. 7-9.

[29] E. REDWAN-R. FRIEDRICH, *A comprehensive reference guide to the Palestinian security and justice sectors*, Geneva Centre for Security Sector Governance, 2023, pp. 105-106.

[30] TREND MICRO RESEARCH TEAM, *Operation Arid Vyper, Bypassing the Iron Dome*, Trend Micro Inc., 2015, pp. 1-31.

sociale decisamente più sofisticate [31]. Ma il vero salto di qualità lo si ebbe a partire dal 2018, quando un elevato numero militari israeliani fu contattato sui social network – Facebook e Whatsapp in testa, spesso da profili hackerati appartenenti a giovani donne – ed indotto a scaricare due applicazioni di *dating* che apparivano legittime ed erano presenti persino all'interno di *Google Play Store*. Una volta installate, tali app (*WinkChat* e *GlanceLove*) consentivano ad Hamas di avere accesso alla posizione del dispositivo mobile, alla lista dei contatti e di utilizzare microfoni e fotocamere per ascoltare e guardare [32]. Similmente, e sempre nel 2018, gli operatori delle IDF furono contattati per scaricare l'applicazione denominata *Golden Cup*, che prometteva (ed in effetti forniva un servizio eccellente) di mostrare risultati ed highlights delle partite del mondiale di calcio che si teneva in Russia [33]. Anche in questo caso, l'app era presente nel *Play Store* di *Google* e appariva del tutto legittima. I funzionari delle forze armate israeliane dichiararono l'operazione di Hamas un fallimento, in quanto soltanto un centinaio di militari avevano effettivamente installato le applicazioni malevole e si riteneva dunque che l'organizzazione palestinese non avesse potuto avere accesso ad informazioni sensibili.

Quello stesso anno, Hamas si segnalò anche per la conduzione di un'operazione cibernetica identica alle precedenti ma avente rilevanti implicazioni psicologiche. Ancora una volta, infatti, gli hacker dell'organizzazione utilizzarono profili illegittimi sui social network, prendendo a bersaglio la popolazione civile e inducendo le vittime a scaricare l'applicazione nota come *Red Alert* (un'app realmente esistente che segnala agli israeliani i bombardamenti missilistici nemici sul territorio del paese). In realtà si trattava di una riproduzione fedele del software legittimo che conteneva uno *spyware* che consentiva ad Hamas l'accesso al dispositivo mobile dell'utente [34]. Ancora una volta, gli apparati di sicurezza israeliani, in collaborazione con aziende private come *ClearSky* (che aveva scoperto il *malware*), riuscirono a limitare i danni. Ovviamente, il fatto che la popolazione civile non potesse riporre la propria fiducia nei software che erano stati creati proprio per salvaguardarne il più possibile la sicurezza aveva anche discrete ripercussioni nella sfera psicologica.

---

[31] S. HANDLER, *op. cit*., p. 13.

[32] O. HOLMES, *Israel: Hamas created fake dating apps to hack soldiers' phones*, in *The Guardian*, 3 luglio 2018.

[33] REUTERS, *Israel says Hamas tried to snare soldiers in World Cup cyber trap*, https://www.reuters.com/article/technology/israel-says-hamas-tried-to-snare-soldiers-in-world-cup-cyber-trap-idUSKBN1JT247/, 3 luglio 2018.

[34] Y. MELMAN, *Hamas attempted to plant a spyware in 'Red Alert' rocket siren app*, in *The Jerusalem Post*, https://www.jpost.com/arab-israeli-conflict/hamas-attempted-to-plant-spyware-in-red-alert-rocket-siren-app-564789, 14 agosto 2018.

Per quanto concerne invece le operazioni d'influenza, esse comprendono quelle cosiddette di *hack-and-leak*, ovvero il furto e la diffusione di informazioni compromettenti, ma anche tutte quelle azioni di deturpazione o sabotaggio dei siti internet e delle pagine web, oltre ovviamente alle campagne sui social network. Nel 2014, a seguito dell'operazione delle forze armate israeliane denominata *Protective Edge*, condotta nella Striscia di Gaza, i militanti di Hamas resero noto di essere riusciti a compromettere diversi computer delle IDF e diffusero alcuni video degli scontri armati tra i regolari di Tel Aviv e gli irregolari palestinesi [35]. Nel corso della stessa *Protective Edge*, diversi siti del governo israeliano subirono attacchi di *Distributed Denial of Service* (DDoS), che li resero temporaneamente inaccessibili agli utenti, e furono trafugati e diffusi dati personali appartenenti a cittadini dello Stato Ebraico [36]. Tali operazioni cibernetiche risultavano utili per creare nell'opinione pubblica israeliana un diffuso senso di insicurezza ed impotenza ed al contempo per mostrare a tutti, palestinesi compresi, le abilità informatiche di Hamas.

L'organizzazione, così come i suoi rivali, ha poi ampiamente sfruttato i social network per diffondere la propria narrazione degli eventi. Per farlo, essa ha richiesto il contributo della popolazione palestinese, pubblicando persino un video con le linee guida da seguire per ottenere contenuti propagandisticamente efficaci: non dovevano essere presenti immagini di missili o armi localizzabili nella Striscia di Gaza, era necessario menzionare ripetutamente i "civili innocenti" e non era sbagliato mostrare *frame* di persone ferite [37].

In effetti, il contributo della popolazione era necessario anche per il successo di altre tipologie di attacco informatico, come ad esempio i DDoS, ed Hamas non mancava di fare appello ai cosiddetti "hacktivist" o agli "hacker patriottici" da tutto il mondo perché collaborassero alle operazioni contro Israele.

Per ciò che riguarda Hezbollah, il gruppo è considerato capace di condurre diverse tipologie di attacco informatico e di sfruttare diverse tecnologie, anche sofisticate. Ciò è piuttosto curioso se si considera che si tratta di un'organizzazione paramilitare, ma può essere spiegato facilmente dal rapporto che essa intrattiene con l'Iran, che ha investito molto nell'addestramento – anche cibernetico – di questa formazione.

---

[35] B. TUFFT, *Hamas claims it hacked IDF computers to leak sensitive details of previous operations*, in *The Independent*, https://www.independent.co.uk/news/world/middle-east/hamas-claims-it-hacked-idf-computers-to-leak-sensitive-details-of-previous-operations-9923742.html, 14 dicembre 2014.

[36] A. ROY, *Cyber Infiltration During Operation Protective Edge*, in *Forbes*, https://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/, 12 agosto 2014.

[37] S. FOWLER, *Hamas and Israel step up cyber battle for hearts and minds*, in *BBC News*, https://www.bbc.com/news/world-middle-east-28292908, 15 luglio 2014.

Come Hamas, anche Hezbollah risultava particolarmente attiva nell'ambito della raccolta di dati per l'intelligence ed in quello della propaganda e delle operazioni di influenza. Per quanto attiene alle prime, tra il 2012 ed il 2015 l'organizzazione dette inizio alla campagna denominata *Volatile Cedar*, volta a trafugare informazioni sensibili dai bersagli israeliani tramite l'impiego di un *malware* appositamente configurato e noto come *Explosive*. La tipologia dell'attacco e lo scarso livello di propagazione del virus rappresenterebbero il principale indizio a dimostrazione delle motivazioni politiche – dunque non finanziarie – della campagna [38]. Nello stesso periodo, ed in particolare a partire dal 2015, la APT (*Advanced Persistent Threat*) nota come *Lebanese Cedar*, collegata ad Hezbollah, ha sfruttato lo stesso malware (*Explosive*) e il *WebShell* denominato *Caterpillar 2.0*, ovvero uno script in grado di fornire accesso remoto permanente al sistema compromesso, per condurre operazioni di intelligence a livello globale [39].

Hezbollah è poi risultato estremamente attivo sui social network nel diffondere la propria narrazione degli eventi, nello screditare i nemici, nel mostrare alla popolazione libanese quanto di buono stava facendo in ambito civile per aumentare i propri consensi e persino per il reclutamento. In aggiunta, profili riconducibili all'organizzazione pubblicavano contenuti in diverse lingue, compreso l'ebraico, con l'obiettivo di rivolgersi anche alle opinioni pubbliche di altri paesi e di demoralizzare i civili israeliani che fossero malauguratamente incappati in un video che mostrava le sofferenze inflitte agli operatori delle IDF [40]. In ultimo, anche Hezbollah ha sfruttato falsi profili Facebook che raffiguravano giovani donne per indurre i bersagli a scaricare applicazioni contenenti *spyware* o altri software malevoli che consentissero all'organizzazione di tracciarli e di accedere ai loro dispositivi [41].

Osservando le operazioni di Hezbollah nel dominio cibernetico, è possibile stabilire la strategia generale seguita dalla formazione paramilitare. Essa combina i propri interessi con quelli dell'Iran, paese che ne sostiene attivamente l'operato sia in termini finanziari che militari. Per questo motivo, le principali vittime degli attacchi informatici di Hezbollah sono israeliane oppure occidentali. Il ricorso allo strumento cibernetico consente all'organizzazione di mantenersi spesso al di sotto della soglia di sicura attribuzione e di evitare eventuali rappresaglie, anche armate. Le operazioni di influenza, invece, sono orientate

---

[38] CHECK POINT, *Volatile Cedar, Threat Intelligence and Research*, Check Point Ltd., 2015.

[39] CLEARSKY, *Lebanese Cedar APT, Global Lebanese Espionage Campaign Leveraging Web Servers*, ClearSky Cybersecurity Ltd., 2021.

[40] D. BYMAN-E. MCCALEB, *Understanding Hamas's and Hezbollah's Uses of Information Technologies*, CSIS Brief, Center for Strategic and International Studies, 2023, pp. 3-4.

[41] *Ibidem*.

da un lato a screditare e porre pressione psicologica sui nemici, in particolare Israele, e dall'altro ad aumentare la propria influenza all'interno della società libanese, mostrando i risultati ottenuti in ambito militare e civile. Seppur in un contesto diverso da quello palestinese, l'operato di Hezbollah non è dissimile da quello di Hamas. Ciò che differenzia le due formazioni paramilitari sono gli obiettivi. Se a livello propagandistico entrambe si rivolgono ad un audience globale, ricercando consensi interni ed esterni, per quanto riguarda le operazioni di spionaggio, Hezbollah non si è limitata a prendere di mira soltanto Israele, arrivando a colpire anche in Occidente e nel mondo arabo.

4. Iran: lo strumento cibernetico come minaccia asimmetrica

La Repubblica Islamica dell'Iran è un attore estremamente rilevante in ambito cibernetico, risultando un rivale decisamente più temibile rispetto ad Hamas e Hezbollah per la sicurezza informatica di Israele. Teheran ha cominciato ad investire in tale settore soprattutto a seguito di due eventi dalla portata dirompente per il regime, ovvero le proteste popolari che seguirono l'esito delle elezioni del 2009 ed il danneggiamento delle centrifughe per l'arricchimento dell'uranio provocato dalla diffusione del *malware* noto come *Stuxnet* nel 2010 [42]. Ciononostante, non esiste un documento che possa essere considerato alla stregua di una vera e propria strategia in ambito cibernetico, o almeno non è mai stato reso pubblico da parte delle autorità di Teheran.

La comunità degli esperti sembra essere divisa rispetto al reale potenziale informatico della Repubblica Islamica. Alcuni ritengono che, nonostante gli innegabili progressi degli ultimi quindici anni, l'Iran non abbia le capacità per rappresentare una seria minaccia agli interessi cibernetici più delicati dei propri rivali – Israele e Stati Uniti in testa – principalmente a causa degli endemici problemi che affliggono il regime e ne minano lo sviluppo anche in altri settori. Altri, invece, ritengono che le capacità e le ambizioni dell'Iran siano tali da poter collocare il paese tra quelli più avanzarti a livello informatico, dietro soltanto ai pesi massimi del sistema, come gli USA, la Cina o il Regno Unito. Ciò che certamente non si può discutere è la mole di investimenti che il regime ha riservato allo sviluppo del settore, che è incrementata costantemente negli ultimi anni [43]. Così come lo sforzo prodotto dalle autorità per creare le istituzioni e gli apparati in grado di implementare nella maniera più efficace possibile una

[42] C. FREILICH, *The Iranian Cyber Threat, The Institution and Praxis of Iran's Cyber Strategy*, Memorandum 230, Institute of National Security Studies, 2024, p. 5.

[43] *Ivi*, p. 26.

strategia cibernetica nazionale. Secondo il *National Cyber Power Index* del 2022, pubblicato dal Belfer Center di Harvard, l'Iran si colloca al decimo posto tra le potenze globali in ambito cibernetico [44].

A livello strategico, la Repubblica Islamica sfrutta gli strumenti tipici del dominio *cyber* a supporto della propria linea politica e dunque come mezzi asimmetrici di confronto con i propri rivali: Israele, gli Stati Uniti e i paesi arabi che hanno normalizzato i propri rapporti con lo Stato Ebraico e che, in ottica iraniana, contribuiscono a sostenerne lo sforzo bellico. Sono proprio tali paesi a rappresentare, secondo gli esperti di *Microsoft*, gli obiettivi privilegiati dell'assertività cibernetica di Teheran [45]. Al loro interno, la Repubblica Islamica sembra interessata a bersagli piuttosto eterogenei, con il 19% degli attacchi condotti contro istituti educativi e di ricerca, l'11% contro imprese ed istituzioni attive nel settore IT, il 7% contro uffici governativi, probabilmente per la raccolta di informazioni di intelligence, sia strategica che tecnologica [46].

In generale, Teheran mantiene una postura piuttosto aggressiva e le operazioni nel dominio cibernetico consentono alla Repubblica Islamica di colpire i propri avversari senza il rischio di subire ritorsioni militari, spesso mantenendosi al di sotto della soglia di attribuzione. In un documento dello Stato Maggiore delle forze armate iraniane del luglio del 2020, il paese si riservava il diritto di rispondere ad operazioni cibernetiche offensive, anche tramite il ricorso alla forza nei domini tradizionali. In aggiunta, nel testo si affermava che qualunque azione informatica avversaria, indipendentemente dall'impatto, sarebbe stata considerata a tutti gli effetti come una violazione della sovranità dell'Iran [47]. In buona sostanza, anche in ambito cibernetico, esiste il dualismo tipico del pensiero strategico della Repubblica Islamica, laddove da un lato si persegue il mantenimento di una sicurezza regionale con implicazioni favorevoli al paese e dall'altro vi è il tentativo di proteggere ed esportare la Rivoluzione.

È proprio per questi motivi che anche l'Iran conduce sia operazioni di intelligence che di influenza, tentando persino di interferire nei processi elettorali dei paesi percepiti come nemici. A livello offensivo, la Repubblica Islamica è dunque ritenuta in grado di condurre azioni di *Computer Network Attack* (CNA), *Computer Network Exploitation* (CNE) e *Computer Network Information* (CNI). La costruzione di tali capacità si è articolata in tre fasi differenti: la

---

[44] J. VOO-I. HEMANI-D. CASSIDY, *National Cyber Power Index 2022*, Report, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2022, p. 9.

[45] MICROSOFT THREAT INTELLIGENCE, *Microsoft Digital Defense Report 2024*, Microsoft, 2024, p. 15.

[46] *Ibidem*.

[47] THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, *Cyber Capabilities and National Power: A Net Assessment*, IISS, 2022, p. 116.

prima, che risale al periodo compreso tra gli anni 2009 e 2011, è relativa alla presa di coscienza delle autorità rispetto alla necessità di sviluppare il potenziale del paese in ambito cibernetico. La seconda, risalente al periodo compreso tra il 2012 ed il 2018, ha visto la creazione dell'impianto istituzionale che si sarebbe occupato delle attività informatiche offensive e della cybersecurity della Repubblica Islamica e l'avvio di un'intensa collaborazione con la Federazione Russa e la Cina avente l'obiettivo di completare la transizione da una postura puramente difensiva in ambito cibernetico alla costruzione di capacità veramente offensive. La terza fase, che risale al periodo successivo al 2019, ha registrato l'imponente espansione del potenziale di attacco dell'Iran, ora in grado di colpire i propri nemici ovunque essi si trovino [48].

Per quanto riguarda siffatte capacità offensive, la Repubblica Islamica si è segnalata, nel corso degli anni, per l'ampia gamma di operazioni che è stata sospettata di aver condotto. In risposta alla scoperta di *Stuxnet*, Teheran condusse una serie di attacchi DDoS contro il sistema bancario statunitense. Nel 2012, l'Iran dimostrò di aver sensibilmente migliorato le proprie capacità, quando colpì la compagnia saudita *Aramco* con un *wiper* noto come *Shamoon* che infettò ben 30.000 dispositivi [49]. Il paese è stato in grado di attaccare imprese in Israele e negli Stati Uniti e persino di prendere il controllo di una diga nello Stato di New York [50]. Una delle campagne più devastanti che la Repubblica Islamica è stata in grado di imbastire è quella che risale al 2022, quando gli hacker del regime colpirono con una serie di attacchi le istituzioni albanesi, colpevoli di avere accettato di ospitare diversi oppositori degli ayatollah. Il piccolo paese balcanico reagì con risolutezza e interruppe le relazioni diplomatiche con Teheran, prendendo addirittura in considerazione l'idea di fare appello all'art. 5 dell'Alleanza Atlantica, richiedendo un intervento in sua difesa dei paesi membri [51]. Negli ultimi anni, l'Iran si è specializzato soprattutto nelle operazioni relative agli ambienti *cloud* ed ha fatto ampio ricorso a strumenti sviluppati *ad hoc*, dimostrando un eccellente livello di sofisticatezza [52]. Cosa che ha permesso agli apparati di Teheran di essere un passo avanti rispetto alle vittime designate, soprattutto vista l'abilità dei primi nello sfruttare rapidamente le nuove vulnerabilità che via via sono emerse. È interessante notare come, a

[48] C. FREILICH, *op. cit.*, pp. 30-31.

[49] THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, *op. cit.*, p. 120.

[50] REUTERS, *Iranian hackers infiltrated computers of a small US dam, says report*, in *The Guardian*, https://www.theguardian.com/us-news/2015/dec/22/iranian-hackers-infiltrated-computers-of-small-us-dam-says-report, 22 dicembre 2015.

[51] C. FREILICH, *op. cit.*, p. 41.

[52] MICROSOFT THREAT INTELLIGENCE, *Microsoft Digital Defense Report, Building and improving cyber resilience*, Microsoft, 2023, p. 66.

partire dal 2022, si sia registrato un netto calo delle operazioni di CNA iraniane (che sfruttavano soprattutto *ransomware*) in favore di quelle di CNI [53]. Un'altra tendenza che gli esperti hanno potuto evidenziare, sempre relativa alle attività offensive vere e proprie, è quella relativa all'intenzione di ottenere guadagni finanziari dalle operazioni cibernetiche, almeno a partire dal 2023 [54].

A livello di intelligence, e dunque di intercettazione e raccolta di dati, la Repubblica Islamica ha dimostrato di avere un buon potenziale, essendo riuscita a penetrare e compromettere diversi sistemi in tutto il mondo, compresi quelli di alcune istituzioni della difesa statunitensi. Come si è visto in precedenza, anche gli enti deputati alla ricerca ed all'educazione sono spesso presi di mira dal regime di Teheran, che si è distinto per i furti di proprietà intellettuale. Nel 2018 fu reso noto che ben 76 istituti universitari collocati principalmente negli Stati Uniti ed in Israele erano stati compromessi dagli hacker iraniani [55].

Secondo alcuni esperti, però, le capacità di Teheran non sono paragonabili a quelle dei propri avversari e non consentono alla Repubblica Islamica di rappresentare una minaccia per i sistemi informatici maggiormente sensibili, vista la scarsa sofisticatezza delle operazioni iraniane. Probabilmente, il rapporto di collaborazione con la Federazione Russa, che si estende anche all'ambito cibernetico, potrebbe migliorare le capacità d'intelligence informatica di Teheran [56]. In aggiunta, a giudicare dalla lunga cronologia di tentativi di compromissione attribuiti alla Repubblica Islamica, sarebbe un errore sottovalutarne eccessivamente il potenziale a livello di raccolta di informazioni, in quanto è possibile notare una notevole continuità nelle operazioni di questo tipo, estesa a tutti gli anni Dieci e Venti del XXI secolo.

L'Iran si distingue invece nel campo delle azioni di *Computer Network Information* (CNI), ovvero tutte quelle attività cibernetiche relative all'ambito cognitivo ed alle operazioni di influenza. In alcuni contesti esse hanno mostrato un ottimo grado di coordinazione con gli attacchi informatici, come nel caso della campagna contro l'Albania, quando un gruppo hacker iraniano noto come *HomeLandJustice* – considerato anche responsabile di alcuni dei suddetti attacchi – ha creato diversi account sui social network ed un sito internet intesi a diffondere la narrazione di Teheran [57].

---

[53] *Ivi*, p. 49.

[54] MICROSOFT THREAT INTELLIGENCE, *Microsoft Digital Defense Report 2024*, cit., p. 17.

[55] SKY NEWS, *UK universities among 76 targeted by hackers*, in *Sky News*, https://news.sky.com/story/uk-universities-among-76-targeted-by-hackers-11480844, 27 agosto 2018.

[56] THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, *op. cit.*, p. 117.

[57] AMERICA'S CYBER DEFENSE AGENCY, *Iranian State Actors Conduct Cyber Operations Against the Government of Albania*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a, 23 settembre 2022.

In generale, l'obiettivo delle operazioni di influenza parrebbe essere quello di amplificare le azioni dannose considerate meno sofisticate. Nel corso degli anni, poi, esse hanno contribuito a sostenere le posizioni del regime al potere, diffondendo narrazioni intese a supportare la causa palestinese, a screditare Israele ed a spaventarne la popolazione, a contrastare la normalizzazione dei rapporti tra Tel Aviv ed i paesi del Golfo ed a fomentare le minoranze sciite che abitano questi ultimi. In aggiunta, l'Iran ha ripetutamente tentato di condurre operazioni di influenza rivolte contro i paesi occidentali, in quella che Teheran pareva considerare una rappresaglia per i tentativi di sovvertire il regime ritenuti eterodiretti dagli Stati Uniti e dai loro alleati [58]. Non a caso, anche diversi paesi membri della NATO sono risultati vittima di azioni volte ad influenzarne le popolazioni ed a screditarne gli organi di stampa – ed i giornalisti – considerati ostili al governo della Repubblica Islamica [59].

Nel condurre operazioni di questo tipo, Teheran si è rivolta anche ad attori che non hanno un legame diretto con il governo, ovvero non sono parte degli apparati di sicurezza iraniani. Questo processo di *outsorcing* ha coinvolto formazioni paramilitari allineate con gli interessi degli ayatollah, come Hezbollah, ma anche media e giornalisti che sono considerati compiacenti con le narrazioni del governo di Teheran [60].

Infine, è noto che la Repubblica Islamica abbia tentato di interferire con il regolare svolgimento delle elezioni di alcuni paesi, ed in particolare con quelle statunitensi del 2020 e del 2024, tramite campagne di influenza cibernetica [61].

Per quanto attiene al sistema delle istituzioni iraniane che si occupano di agire all'interno del dominio cibernetico e della cybersecurity del regime, esso si articola in maniera piuttosto complessa. A livello politico, il *Supreme Council for Cyberspace*, di cui anche il Presidente è parte, rappresenta la principale autorità di coordinamento legislativo e decisionale. Esso si compone di 27 membri provenienti dalle istituzioni governative, incluse le forze armate e gli apparati di sicurezza, e dalla società civile. Tale organo implementa le proprie decisioni tramite il *National Cyberspace Center* (NCC), creato a tale scopo nel 2013. In posizione subordinata rispetto a tali istituzioni si trovano diverse agenzie, alcune delle quali deputate esclusivamente alla sicurezza cibernetica della Repubblica Islamica ed altre, apparentemente, dotate di un buon potenziale offensivo.

---

[58] MICROSOFT THREAT INTELLIGENCE, *Microsoft Digital Defense Report, Building and improving cyber resilience*, *op. cit.*, p. 67.

[59] *Ivi*, p. 68.

[60] *Ivi*, p. 69.

[61] Cfr. *ex multis* FBI NATIONAL PRESS OFFICE, *Joint ODNI, FBI and CISA Statement on Iranian Election Influence Efforts*, https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts, 19 agosto 2024.

Tra esse è utile ricordare la *National Passive Defense Organization*, responsabile della difesa delle infrastrutture critiche e della società civile, la unità informatiche della polizia, le unità informatiche dei Guardiani della Rivoluzione (IRGC), che possiedono capacità di attacco, il *Cyber Defense Command* delle forze armate, spesso coinvolto anche in operazioni di natura offensiva ed il Ministero dell'Intelligence e della Sicurezza (MOIS), a sua volta in grado di condurre azioni di attacco [62].

Per quanto concerne queste ultime, secondo il team di *Microsoft Threat Intelligence*, gli organismi maggiormente pericolosi sarebbero proprio il MOIS e le Guardie della Rivoluzione, che controllerebbero diverse unità classificate come APTs. Tra esse è possibile elencare *Cotton Sandstorm*, *Mango Sandstorm*, *Pink Sandstorm*, *Mint Sandstorm* (anche nota come *Charming Kitten* o APT-35), *Helix Kitten* (anche nota come APT-34), *Peach Sandstorm* (anche nota come *Elfin Team*, APT-33 o *Refined Kitten*), ecc. Alcune di queste unità sarebbero direttamente coinvolte anche in operazioni di influenza [63].

5. Il conflitto in Medio Oriente da una prospettiva cibernetica

Sebbene sia ancora prematuro pretendere di fornire una descrizione completa dei drammatici eventi che tuttora sono in corso nel quadrante geopolitico levantino, è certamente possibile esaminare alcuni degli aspetti che hanno caratterizzato i primi momenti del conflitto, almeno da una prospettiva cibernetica.

Già nelle primissime ore del 7 ottobre, durante l'azione terroristica di Hamas entro i confini dello Stato Ebraico, si registrò un notevole incremento degli attacchi informatici rivolti verso Israele. *Check Point* osservò un aumento delle attività malevole contro Tel Aviv pari al 18% rispetto ai giorni precedenti con un'intensificazione delle operazioni digitali dirette verso istituzioni governative e militari pari al 52% [64]. Tali attività si articolavano principalmente in attacchi di tipo DDoS, in azioni di *hack and leak* e in deturpazioni di pagine web israeliane. Per quanto concerne i primi, Hamas ricorse alla collaborazione di numerosi gruppi di hacktivist tendenzialmente islamisti, come quelli denominati *Ghosts of Palestine* oppure *Team_Insane_Pakistan*. Tra i bersagli dell'azione

---

[62] THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, *op. cit.*, pp. 116-117.

[63] MICROSOFT THREAT INTELLIGENCE, *Iran surges cyber-enabled influence operations in support of Hamas*, Microsoft, 2024, p. 7.

[64] CHECK POINT RESEARCH, *The Iron Swords War – Cyber Perspectives from the First 10 Days of War in Israel*, https://blog.checkpoint.com/security/the-iron-swords-war-cyber-perspectives-from-the-first-10-days-of-the-war-in-israel/, 18 ottobre 2023.

di tali formazioni vi furono anche la Banca d'Israele, la Knesset e la compagnia di servizi per telefonia mobile *Cellcom*. I risultati di tali attività malevole non furono particolarmente gravi.

Per ciò che riguarda le operazioni di *hack and leak*, ovvero il furto e poi la diffusione di dati personali o sensibili a scopi propagandistici, furono diversi i siti colpiti, compreso quello del prestigioso istituto universitario denominato *Ono Academic College*, di cui furono compromesse anche le telecamere a circuito chiuso installate nel campus [65]. Invece, le operazioni di deturpazione riguardarono non soltanto alcune pagine web ma anche i cartelloni pubblicitari elettronici. Nei giorni immediatamente successivi all'attacco terroristico di Hamas, alcuni di essi trasmisero immagini a sostegno dell'organizzazione [66].

Nel corso dello stesso mese di ottobre, si registrarono anche operazioni maggiormente sofisticate dirette contro Israele. In particolare, un gruppo di hacktivist filo-palestinesi noto come *AridViper* o APT-C-23, e quasi certamente collegato ad Hamas, sfruttò un *wiper* in grado di compromettere dispositivi con sistema operativo *Linux* che ribattezzò "BiBi" (dal soprannome del Primo Ministro israeliano Benjamin Netanyahu), potenzialmente molto efficacie [67]. In realtà, il *malware* fu rinvenuto anche in dispositivi dotati di sistema operativo *Windows*, a dimostrazione delle capacità del gruppo, ma, per quanto è dato sapere, le operazioni di *AridViper* fallirono nella maggior parte dei casi, principalmente per merito della resilienza dell'ecosistema – pubblico e privato – di cybersicurezza israeliano.

È di assoluto interesse notare come, già in questa fase del conflitto, fu possibile registrare un incremento delle attività informatiche malevole dirette contro lo Stato Ebraico anche da parte di attori esterni al quadrante geopolitico mediorientale, come il network di hacktivist russi unito sotto la sigla *KillNet* [68], o quello, sempre legato al Cremlino, noto come *Anonymous_Sudan*.

In generale, si registrarono operazioni cibernetiche contro Israele da parte di gruppi provenienti dall'Iran, dall'Indonesia, dal Qatar, dalla Turchia e dalla

---

[65] *Ibidem*.

[66] H. FIELD, *Billboards in Israel were briefly hacked to display pro-Hamas messages as cyberwar ramps up*, in *CNBC*, https://www.cnbc.com/2023/10/12/billboards-in-tel-aviv-briefly-hacked-to-display-pro-hamas-messages.html, 12 ottobre 2023.

[67] R. LAKSHMANAN, *Pro-Hamas Hacktivists Targeting Israeli Entities with Wiper Malware*, in *The Hacker News*, https://thehackernews.com/2023/10/pro-hamas-hacktivists-targeting-israeli.html, 30 ottobre 2023.

[68] ANSA, *Attacchi hacker a Israele sono dei filorussi Killnet*, in *ANSA*, https://www.ansa.it/canale_tecnologia/notizie/cybersecurity/2023/10/09/attacchi-hacker-a-israele-sono-dei-filorussi-killnet_5dc78c5a-be03-47e7-bba8-b7f7b357a2cd.html, 10 ottobre 2023.

Malesia, mentre paesi come gli Stati Uniti, il Canada, l'Australia, la Germania e l'India contribuirono alla difesa informatica dello Stato Ebraico [69].

Ad ogni modo, nelle fasi iniziali del conflitto, i gruppi hacker filo-palestinesi si segnalarono anche per un paio di interessanti operazioni che presero di mira le applicazioni maggiormente diffuse tra i civili israeliani per la segnalazione di attacchi missilistici (che, peraltro, nei primissimi giorni di guerra furono più di 5.000). Nel dettaglio, l'organizzazione nota come *AnonGhost* fu in grado di compromettere, sfruttandone una vulnerabilità non ancora nota, l'app denominata *Red Alert: Israel*. L'azione consentì al gruppo di accedere a diverse informazioni, di intercettare le richieste degli utenti e di inviare falsi allarmi sui dispositivi di questi ultimi, inclusa un'allerta nucleare. Questo non fu l'unico episodio. Nella prima settimana di guerra, un sito malevolo cominciò a pubblicizzare un'applicazione legittima nota, anch'essa, come *RedAlert*. Il link presente nella pagina web indirizzava l'utente al *Play Store* di *Google*, ma l'app che veniva scaricata sul dispositivo del malcapitato era una versione che, pur riproducendo fedelmente il software legittimo, conteneva codice malevolo. In tale caso, esso consentiva agli hacker palestinesi di accedere ad una grandissima quantità di informazioni presenti nel dispositivo che era stato infettato [70].

Tra le azioni intraprese da Israele per contrastare l'ondata di attacchi cibernetici di cui fu vittima nella fase iniziale del conflitto, una di quelle che ebbero maggior impatto fu la completa disconnessione della Striscia di Gaza dalla rete internet globale, operata principalmente tramite il bombardamento massiccio dell'infrastruttura e facilitata dal completo controllo che, come si è visto in precedenza, Israele esercita sul sistema di comunicazioni informatiche palestinese. Il blackout ebbe inizio il 27 ottobre 2023 e sollevò immediatamente la perplessità – ed in alcuni casi le polemiche – degli osservatori internazionali e delle organizzazioni umanitarie in merito alla legalità di attacchi diretti a quella che viene ormai considerata un'infrastruttura critica [71].

Chiaramente, la risposta militare non fu l'unica azione adottata dallo Stato Ebraico. *Cloudflare* registrò infatti un contestuale aumento degli attacchi di tipo

---

[69] N. SINGH-S. BAJEJE, *Hacktivism or Cyberwarfare? Decoding the Motivations Behind Cyber Attacks Targeting Israel*, in S. RAJAGOPAL-K. POPAT-D. MEVA-S. BEJEJE-P. MUDHOLKAR (ed.), *Artificial Intelligence Based Smart and Secured Applications*, Springer, Cham, 2025, pp. 206-232.

[70] B. DARCHE-A. BOURSALIAN-J. CASTRO, *Malicious "Red Alert – Rocket Alerts" application targets Israeli phone calls, SMS, and user information*, in *The Cloudflare Blog*, https://blog.cloudflare.com/malicious-redalert-rocket-alerts-application-targets-israeli-phone-calls-sms-and-user-information/, 14 ottobre 2023.

[71] M. MILLER, *Internet blackout in Gaza as Israel expands operations*, in *Politico*, https://www.politico.com/news/2023/10/27/internet-blackout-gaza-israel-hamas-war-00124029, 27 ottobre 2023.

DDoS diretti contro le pagine web palestinesi (almeno fino a quando era disponibile una connessione internet nella Striscia di Gaza), in concomitanza con l'avvio della campagna aerea in risposta ai drammatici eventi del 7 ottobre [72].

Ad ogni buon conto, con il passare delle settimane, le attività cibernetiche malevole collegate al conflitto non si attenuarono, soprattutto quelle diretta contro Tel Aviv. Diverse piattaforme digitali, come Signature-IT che si vide sottratti 16 GB di dati sensibili, istituzioni governative, come gli Archivi di Stato di Israele, istituzioni civili, come le infrastrutture mediche e gli ospedali, oppure gli organi di stampa, furono vittima di attacchi [73]. In aggiunta, fu chiaro fin da subito che gruppi hacker iraniani, come ad esempio *CyberAv3ngers*, stessero attivamente partecipando al conflitto cibernetico in corso. Per tutta la durata del 2023 e del 2024, poi, Teheran tentò di raccogliere informazioni sui propri nemici israeliani tramite la compromissione dei sistemi di telecamere a circuito chiuso e attraverso diversi tentativi di corruzione di cittadini dello Stato Ebraico – anche e soprattutto se appartenenti alle IDF – tramite i social network [74].

Similmente, non si attenuarono neppure gli attacchi di tipo DDoS o le deturpazioni dei siti. Si registrarono attività di questo tipo da parte di tutti gli attori coinvolti ma Tel Aviv subì senza dubbio la stragrande maggioranza delle azioni malevole [75].

Per quanto concerne i flussi finanziari, a partire dal 7 ottobre 2023 furono scoperti e chiusi oltre 100 conti in criptovalute collegati in vario modo ad Hamas, prevalentemente sulla piattaforma *Binance*. Alcuni dei finanziamenti provenivano, prevedibilmente, dall'Iran [76].

Ben presto, si evidenziò un allargamento del conflitto, con Israele che dette avvio ad una campagna di bombardamenti in territorio libanese, con l'obiettivo di deteriorare il potenziale militare di Hezbollah, responsabile di aver condotto diversi attacchi missilistici contro obiettivi situati nello Stato Ebraico sin dal momento dell'*escalation* militare nella Striscia di Gaza. In questo teatro bellico, le operazioni cinetiche israeliane furono accompagnate da attacchi cibernetici. In generale, gli apparati di sicurezza di Tel Aviv furono particolarmente abili ad infiltrarsi nei sistemi di comunicazione dei militanti di Hezbollah e proprio

---

[72] O. YOACHIMIK-J. PACHECO, *Cyber attacks in the Israel-Hamas war*, in *The Cloudflare Blog*, https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/, 23 ottobre 2023.

[73] T. PAVEL, *Avoiding a 'digital 7th October': a study on cyberwarfare against Israel during the October 2023 war*, in *Contemporary Military Challenges*, 2024, vol. 26, n. 3, pp. 95-112.

[74] *Ibidem*.

[75] A. VU-A. HUTCHINGS-R. ANDERSON, *Yet Another Diminishing Spark: Low-Level Cyberattacks in the Israel-Gaza Conflict*, in *Proceedings of the IEEE European Symposium on Security and Privacy Workshops 2025*, 2025.

[76] T. PAVEL, *Avoiding a 'digital 7th October'*, cit.

in questo ambito nacque quella che fu ribattezzata "*Operation Grim Beeper*". Si trattava di un'azione ibrida, che soltanto marginalmente aveva a che fare con il dominio cibernetico, ma che divenne famosissima in tutto il mondo. Gli operatori dell'intelligence israeliana riuscirono infatti a compromettere i cercapersone ed i walkie-talkie appartenenti ad un numero cospicuo di militanti di Hezbollah, che li utilizzavano perché li ritenevano maggiormente sicuri rispetto al rischio di intercettazioni. Nei dispositivi era stato inserito dell'esplosivo, che fu innescato da remoto tramite un semplice messaggio. L'azione efferata portò alla morte di molti membri dell'organizzazione ed al ferimento di altri, mietendo anche vittime innocenti [77].

Per quanto riguarda Hezbollah, i libanesi condussero alcune operazioni degne di nota nei giorni immediatamente successivi agli attacchi del 7 ottobre. Il gruppo hacker *GreatRift*, collegato all'organizzazione, si attivò per impersonare servizi di emergenza israeliani legittimi dando avvio ad una campagna di phishing con l'obiettivo di indurre i bersagli a scaricare software malevoli nei loro dispositivi. In alcuni casi, i libanesi arrivarono a creare false pagine web per le persone scomparse (Hamas aveva rapito oltre 250 cittadini dello Stato Ebraico), ancora una volta con l'intendo di diffondere *malware* [78].

Ad ogni modo, l'allargamento del conflitto coinvolse in breve tempo anche l'Iran, che da sempre sosteneva attivamente la causa palestinese e che era fortemente sospettato di aver supportato Hamas nella pianificazione e nella realizzazione dell'attacco del 7 ottobre. Senza contare che gli apparati cibernetici della Repubblica Islamica si erano immediatamente attivati per condurre operazioni contro Israele, anche se soprattutto attinenti al campo delle azioni di influenza. Più nel dettaglio, riguardo agli attacchi informatici veri e propri, Teheran aveva preso di mira le infrastrutture critiche rivali tramite l'impiego del *wiper* denominato "*No-Justice*", probabilmente diffuso dal gruppo *Void Manticore*, collegato direttamente con il MOIS [79]. Secondo alcuni esperti, lo stesso "BiBi" sarebbe stato prodotto ed utilizzato da hacker iraniani. In aggiunta, il collettivo noto come *Cyber Av3ngers*, già citato in precedenza, si sarebbe reso responsabile a propria volta di ripetuti attacchi alle infrastrutture critiche israeliane, statunitensi e persino irlandesi [80]. È interessante notare come la Repubblica Islamica abbia fatto

---

[77] J. RATHBONE-M. SEDDON-J. KYNGE, *How Israel's "Operation Grim Beeper" rattled global spy chiefs*, in *The Financial Times*, https://www.ft.com/content/f578b6c0-d534-4a04-ae25-3b97d11b6e71, 28 dicembre 2024.

[78] GOOGLE THREAT INTELLIGENCE, *Tool of First Resort, Israel-Hamas War in Cyber*, Google, 2024, p. 24.

[79] CHECK POINT RESEARCH, *The state of cybersecurity 2025, Top threats, emerging trends and, CISO recommendation*, Check Point Ltd., 2025, p. 12.

[80] *Ivi*, p. 13.

ampio ricorso a gruppi di hacktivist, o presunti tali, con l'obiettivo di nascondere il proprio coinvolgimento mantenendo quella che in gergo viene definita *plausible deniability*. Molto spesso, però, tali gruppi avevano un collegamento diretto con gli apparati di sicurezza di Teheran.

Per quanto riguarda invece le operazioni di influenza, esse possono essere divise in tre fasi distinte. Inizialmente tali campagne potevano essere definite come reattive rispetto agli eventi in corso. La narrazione che veniva diffusa era dunque una risposta agli accadimenti sul campo. Persino il materiale su cui di volta in volta le operazioni si basavano era stato trafugato dagli apparati di intelligence molto tempo prima dell'inizio del conflitto in Medio Oriente e, in alcuni casi, era già stato reso pubblico. La seconda fase vide un netto incremento nel numero degli attori coinvolti nella campagna, tanto da essere ribattezzata dal gruppo di esperti di *Microsoft* "*All-Hands-on-Deck*". In questo frangente, i social media divennero estremamente importanti, così come le impersonificazioni di attivisti israeliani o palestinesi. Si registrò un certo grado di coordinazione con le operazioni cibernetiche di altro tipo, spesso accompagnate da messaggi intesi a generare un effetto psicologico sul bersaglio. Si registrò inoltre il ricorso all'uso di messaggi privati via mail o SMS alla vittima di turno. La terza ed ultima fase della campagna, infine, vide un ampliamento dell'audience delle attività iraniane, che si espanse fino a comprendere anche gli alleati di Tel Aviv, con l'intenzione di isolare Israele [81].

In effetti, gli obiettivi perseguiti da Teheran parevano essere essenzialmente quelli di intimidire e dividere la popolazione dello Stato Ebraico, che al contempo doveva essere screditato agli occhi di tutto il mondo e soprattutto dell'Occidente. Per raggiungerli ed amplificare le proprie narrazioni, Teheran ricorse soprattutto alle tecniche di impersonificazione di attivisti israeliani sui social network, che richiamavano il popolo all'azione contro il governo di Tel Aviv, arrivando persino ad ingaggiare ignari cittadini dello Stato Ebraico per appendere striscioni coerenti con la narrazione della Repubblica Islamica. Inoltre, con molto meno successo, l'Iran ricorse all'impiego dei propri media e di campagne di sensibilizzazione via mail per amplificare ulteriormente il messaggio che intendeva diffondere [82]. Appare a questo punto interessante sottolineare il ruolo crescente dell'intelligenza artificiale (AI) nella conduzione di campagne di influenza, ben dimostrata dalle attività dell'Iran.

Israele, dal canto suo, non risparmiò l'avversario da attacchi nel dominio cibernetico, facendo a propria volta ampio ricorso a gruppi di hacktivist [83]. Nel

---

[81] MICROSOFT THREAT INTELLIGENCE, *Iran surges cyber-enabled influence operations in support of Hamas*, *op. cit.*, pp. 4-11.

[82] *Ivi*, pp. 12-14.

[83] N. SHAH, *What the Israel-Iran conflict revealed about wartime cyber operations*, in

campo della raccolta di informazioni, e dunque dell'intelligence, Teheran ha più volte accusato lo Stato Ebraico di spionaggio informatico, ma è assai difficile trovare riscontri reali, proprio per la natura di questa particolare tipologia di operazioni [84]. È però molto probabile che gli apparati di sicurezza dello Stato Ebraico abbiano condotto – e ancora conducano – ferventi attività in questo ambito. Così come è difficile attribuire ad Israele la serie di attacchi cibernetici diretti contro le infrastrutture energetiche della Repubblica Islamica alla fine del 2023, rivendicati dal gruppo hacker *Predatory Sparrow* [85], che potrebbe avere legami, seppur non dimostrati, con Tel Aviv [86]. Tel Aviv che è risultata attiva anche dal punto di vista delle operazioni di influenza, nel caso iraniano andando forse oltre i principi dell'*hasbara*. Il governo israeliano, così come le forze armate, avrebbero infatti utilizzato proficuamente i propri canali in lingua persiana sui social network, facendo leva su una narrazione che evidenziava la millenaria amicizia tra persiani ed ebrei, scalfita soltanto, negli ultimi quasi cinque decenni, dalle folli idee degli ayatollah. Il tutto condito con più o meno celati riferimenti alla gloriosa storia ed ai costumi di quella che anticamente era la Persia [87].

Infine, per quanto concerne l'intelligenza artificiale, è indubbio che essa abbia avuto un ruolo fondamentale in questo conflitto anche sulla sponda israeliana. Se da un lato la sopravvalutazione delle capacità predittive dei sistemi di AI ha contribuito a determinare il fallimento di intelligence che ha consentito gli attacchi del 7 ottobre, dall'altro armamenti come i droni si sono rivelati assolutamente necessari per la conduzione del conflitto. Basti pensare anche solo alle famose immagini della morte del famigerato leader dell'ala militare di Hamas, Sinwar, identificato tramite l'impiego di un UAV [88]. Tel Aviv ha fatto persino ricorso ad un sistema di *targeting* dei bersagli nella Striscia di Gaza basato sull'intelligenza artificiale, che pone però ulteriori dilemmi etici in quanto privo di un approfondito controllo umano e correlato a politiche permissive rispetto ai cosiddetti danni collaterali (ovvero le vittime innocenti). Sviluppato dall'altrettanto famigerata unità 8200, esso avrebbe identificato 37.000 palestinesi

---

Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/, 30 luglio 2025.

[84] Cfr. *ex multis* E. LYONS, *Meta 'concerned' by Iran telling citizens to stop using WhatsApp, spokesperson says*, in *CBS News*, https://www.cbsnews.com/news/meta-concerned-iran-telling-citizens-stop-using-whatsapp/, 17 giugno 2025.

[85] GOOGLE THREAT INTELLIGENCE, *op. cit.*, p. 25.

[86] N. SHAH, *op. cit.*

[87] M. MARELLI, *'Nel nome di Ciro il Grande', Propagande israeliane a uso e consumo degli iraniani*, in *Limes*, 2025, n. 6, pp. 155-162.

[88] BBC, *IDF drone footage 'shows Sinwar in final moments'*, in *BBC*, https://www.bbc.com/news/videos/c8djz4rn144o, 18 ottobre 2024.

della Striscia di Gaza come possibili bersagli, con il personale militare delle IDF che dedicava in media 20 secondi ad ogni vittima per decidere se autorizzarne l'eliminazione. Il tutto con un indice d'errore del dispositivo di *targeting* pari al 10%, ben noto ai soldati israeliani [89].

6. Conclusione

Il conflitto attualmente in corso in Medio Oriente, cominciato con gli attentati del 7 ottobre condotti da Hamas e proseguito con un'intensa campagna di bombardamenti sulla Striscia di Gaza, poi allargatasi al Libano, all'Iran, allo Yemen ed alla Siria, ha dimostrato ancora una volta, se ve ne fosse bisogno, l'importanza del dominio cibernetico nella conduzione di una guerra.

A giudicare dagli eventi che hanno interessato la regione del Mediterraneo Orientale ed il Levante, ormai non è più possibile pensare di condurre operazioni militari tradizionali senza che esse vengano coordinate con attività offensive o difensive nel campo informatico. E ciò vale sia per attori tecnologicamente avanzanti, come Israele o l'Iran, sia per le formazioni paramilitari come Hamas o Hezbollah. Ciò perché gli attacchi nel dominio cibernetico possiedono un grande potenziale, possono produrre anche danni molto rilevanti, ma consentono di mantenersi al di sotto della soglia di attribuzione e di quella di guerra. Consentono, in sostanza, di controllare l'*escalation* militare e sono dunque strategicamente fondamentali per chiunque voglia evitare di muovere troppo lontano la proverbiale asticella.

Il Mediterraneo è un teatro "caldo" in questa fase storica. La consapevolezza della pericolosità delle azioni nel dominio cibernetico, comprese le operazioni di influenza, in grado di destabilizzare interi paesi, è fondamentale. E lo è anche per noi, che siamo nella sponda europea del *Mare Nostrum*, e quindi tutti interconnessi e vulnerabili.

[89] Y. ABRAHAM, *'Lavender': The AI machine directing Israel's bombing spree in Gaza*, in *+972 Magazine*, https://www.972mag.com/lavender-ai-israeli-army-gaza/, 3 aprile 2024.

Capitolo 6

Politiche di cybersicurezza e implicazioni strategiche: una lettura politologica

Luigi Martino [*], Giampiero Giacomello [**], Oltion Preka [***]

Abstract: A partire dall'analisi dell'attuale quadro delle politiche di governance della cybersicurezza in Italia e in Europa, dei principali attori coinvolti e degli strumenti normativi chiave, la presente indagine intende approfondirne le implicazioni politico-strategiche e offrire un confronto tra l'approccio europeo e quello italiano – con riferimenti ad esperienze di altri Stati membri – evidenziando le peculiarità e le convergenze, nonché l'impatto di tali politiche sui principali settori applicativi (infrastrutture critiche, PMI, settore privato e pubblica amministrazione).

Keywords: Politiche di cybersicurezza – Diritto dell'UE – Perimetro di Sicurezza Nazionale Cibernetica (PSNC) – Resilienza – Sovranità digitale

[*] Ricercatore a tempo determinato tipo a) di Scienza politica, presso il Dipartimento di Scienze Politiche e Sociali dell'Università di Bologna, luigi.martino3@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

[**] Professore associato di Scienza politica, presso il Dipartimento di Scienze Politiche e Sociali dell'Università di Bologna, giampiero.giacomello@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

[***] Assegnista di ricerca presso, il Dipartimento di Scienze Politiche e Sociali dell'Università di Bologna, oltion.preka@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

La sicurezza cibernetica è divenuta un pilastro strategico per la tutela degli interessi nazionali e dello sviluppo economico, sia in Italia che nell'Unione Europea. Negli ultimi anni, i decisori pubblici hanno approntato un'articolata architettura normativa e istituzionale per far fronte alle crescenti minacce digitali, muovendosi su più livelli: dal rafforzamento delle strutture governative interne, alla definizione di strategie nazionali, fino all'adozione di direttive e regolamenti europei sempre più incisivi. L'evoluzione di questo ecosistema normativo riflette la consapevolezza che le minacce cyber, per loro natura transnazionali e ibride, richiedono approcci coordinati e una stretta cooperazione tra settore pubblico e privato [1].

Il capitolo analizza l'attuale quadro delle politiche di governance della cybersicurezza in Italia e in Europa, delineando i principali attori coinvolti e le relative competenze, esaminando gli strumenti normativi chiave – dalla direttiva NIS2 al *Cyber Resilience Act* (CRA), da DORA al *Cybersecurity Act* (CSA) e al neonato *Cyber Solidarity Act* a livello UE, dal Perimetro di Sicurezza Nazionale Cibernetica (PSNC) all'Agenzia per la Cybersicurezza Nazionale (ACN), dalla Strategia Nazionale 2022-2026 fino alla recente l. n. 90/2024 in ambito italiano [2]. Verranno, in particolare, approfondite le implicazioni politico-strategiche di questo complesso quadro: la ricerca di autonomia strategica digitale, il potenziamento della resilienza di sistemi e infrastrutture critiche, le forme di partenariato pubblico-privato, l'approccio alle minacce ibride e l'industrializzazione degli attacchi. Infine, si offrirà un confronto tra l'approccio europeo e quello italiano – con riferimento ad esperienze di altri Stati membri ove pertinente – evidenziando le peculiarità e le convergenze, nonché l'impatto di tali politiche sui principali settori applicativi (infrastrutture critiche, PMI, settore privato e pubblica amministrazione).

---

[1] Per un quadro generale sulla cybersecurity globale si veda ad esempio G. GIACOMELLO (a cura di), *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*, New York, Bloomsbury, 2014.

[2] LISA SERVIZI SRL., *Cybersicurezza: i punti salienti della Legge 90/2024*. Blog Lisa Servizi HSE, 19 marzo 2025 (https://www.lisaservizi.it/legge-n-90-2024-cybersicurezza).

2. Architettura istituzionale e normativa della cybersicurezza in Italia

Negli ultimi anni, l'Italia ha radicalmente ridisegnato la propria governance della cybersecurity, passando da un assetto frammentato ad un modello più centralizzato e coordinato [3]. Un momento cruciale è stato il varo del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), istituito con il d.l. n. 105/2019 (convertito con l. n. 133/2019), il quale definisce una "rete di protezione" attorno alle infrastrutture digitali essenziali per il funzionamento del Paese. Il PSNC individua soggetti pubblici e privati di rilevanza strategica (nei settori come energia, telecomunicazioni, trasporti, finanza, sanità, difesa, ecc.) tenuti al rispetto di stringenti misure di sicurezza, alla notifica di incidenti e a procedure di verifica sulle forniture ICT. Si tratta di un regime parallelo e complementare alla normativa europea NIS, motivato dall'esigenza di tutelare la sicurezza nazionale anche al di là dei servizi essenziali definiti dall'UE [4].

Come osservato, il Perimetro è un sistema in costante evoluzione che oggi coinvolge centinaia di soggetti strategici; nel 2025 è stato aggiornato mediante il d.p.c.m. 4 giugno 2025 n. 111, introducendo nuove categorie di incidenti da segnalare, tra cui accessi non autorizzati con abuso di privilegi, così da rispondere all'evoluzione delle minacce. Attraverso il PSNC, l'Italia ha anticipato alcuni elementi poi ripresi dalla direttiva NIS2, ponendo le basi di un approccio nazionale organico volto alla protezione delle infrastrutture critiche.

Il fulcro dell'architettura istituzionale italiana risiede nell'Agenzia per la Cybersicurezza Nazionale (ACN), istituita nel 2021 (d.lgs. 14 giugno 2021, n. 82, convertito con l. n. 109/2021). L'ACN è l'Autorità nazionale cyber con competenze di coordinamento, attuazione delle strategie di cyber difesa civile, vigilanza su sicurezza delle reti e certificazione, nonché punto di contatto unico per le autorità europee in materia. Essa incorpora il precedente CSIRT italiano (Computer Security Incident Response Team) con funzioni di risposta agli incidenti e opera alle dirette dipendenze della Presidenza del Consiglio dei Ministri. Attorno all'ACN ruota un complesso sistema di governance che include il Comitato Interministeriale per la Cybersicurezza (CIC), organo politico strategico presieduto dal Presidente del Consiglio, incaricato di approvare indirizzi e strategie (come la Strategia Nazionale), e il Nucleo per la Cybersicurezza –

[3] Per un'analisi complessiva, si rimanda al contributo di T.F. Giupponi, *Il quadro della governance della cybersicurezza a livello nazionale*, in questo volume.

[4] A. Cicchinelli-A. Marella, *Governance della cybersecurity in Europa e oltre: analisi comparata tra Italia, Francia, Germania e il modello anglosassone*, in *Rivista Cammino Diritto*, 24 settembre 2025 (disponibile su Cammino Diritto: https://rivista.camminodiritto.it/articolo.asp?id=11188); L. Martino, *Cybersecurity in Italy: Governance, Policies and Ecosystem*, Cham, Springer, 2024.

struttura tecnico-operativa ristretta attivata in caso di crisi cibernetiche. A livello operativo, cooperano inoltre il comparto intelligence (DIS, AISE, AISI) e le forze dell'ordine specializzate (in primis il CNAIPIC della Polizia Postale) per gli aspetti rispettivamente di sicurezza cibernetica offensiva/difensiva e di contrasto al cybercrime. Ne risulta un quadro istituzionale articolato, con numerosi stakeholder e centri decisionali, che richiede di capire chiaramente "chi fa cosa" in ambito cyber per potersi orientare efficacemente. Pur nelle sue specificità, il modello italiano si inserisce infatti nel più ampio contesto europeo ed internazionale, con cui interagisce costantemente in termini di recepimento normativo e di collaborazione strategica [5].

Sul piano normativo interno, oltre al già citato d.lgs. n. 105/2019 (PSNC) e al d.lgs. n. 82/2021 (istitutivo di ACN), meritano attenzione sia la Strategia Nazionale di Cybersicurezza 2022-2026, adottata nel 2022 dal CIC, che la recente l. 4 luglio 2024, n. 90. La Strategia 2022-26, corredata da un dettagliato Piano di implementazione, rappresenta la *road map* pluriennale per rafforzare sicurezza e resilienza cyber del Paese. Il documento individua tre obiettivi fondamentali – Protezione, Risposta e Sviluppo – declinati in 82 misure specifiche, ciascuna con attori responsabili e tempistiche definite. In sintesi, *Protezione* significa difendere gli asset strategici nazionali con un approccio integrato di gestione del rischio e misure normative/tecniche abilitative per una transizione digitale resiliente; *Risposta* attiene alla capacità di rilevare, analizzare e reagire in modo coordinato a minacce, incidenti e crisi cibernetiche, coinvolgendo l'intero ecosistema nazionale (dalle istituzioni alle aziende); *Sviluppo,* infine, riguarda il potenziamento sicuro delle tecnologie digitali e la promozione di competenze, centri di eccellenza e filiere industriali nazionali, così da assicurare al Paese un adeguato livello di autonomia strategica nel settore. Proprio il tema dell'autonomia strategica – ovvero la capacità di ridurre la dipendenza da tecnologie estere e dominare le tecnologie chiave – è uno dei principi cardine della strategia italiana e rientra tra le finalità esplicite del pilastro "Sviluppo", in linea con le analoghe ambizioni europee nell'ambito della sovranità digitale.

La l. n. 90/2024 rappresenta un ulteriore tassello normativo di rilievo, mirato a rafforzare la resilienza cyber del settore pubblico e ad aggiornare il quadro

---

[5] CONFINDUSTRIA & GRUPPO GENERALI, *Rapporto Cyber Index PMI 2024*, II ed., presentato a marzo 2025 (Comunicato Confindustria, 27 marzo 2025: "PMI non raggiungono la sufficienza in gestione dei rischi cyber"); A. CICCHINELLI-A. MARELLA, *Il perimetro di sicurezza nazionale cibernetica: cos'è e come evolve*, in *Agenda Digitale*, 5 agosto 2025 (https://www.agendadigitale.eu/sicurezza/il-perimetro-di-sicurezza-nazionale-cibernetica-cose-e-come-evolve/). Su questo punto, per una prospettiva più generale, si veda anche G. GIACOMELLO, *A Perfect Storm: Privatization, public-private partnership and the security of critical infrastructure*, in G. GIACOMELLO-N. MORO-M. VALIGI (eds), *Technology and International Relations: The New Frontier in Global Power*, Cheltenham, UK, Edward Elgar Publishing Ltd, 2021, pp.173-192.

sanzionatorio penale sui reati informatici. Tale legge – dal titolo *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* – impone una serie di adempimenti stringenti in capo a una vasta platea di soggetti pubblici. In particolare, richiede agli enti pubblici di istituire idonee strutture interne per la sicurezza informatica, con i seguenti compiti UE (a) sviluppo di politiche e procedure di sicurezza, (b) predisposizione di sistemi di analisi preventiva e piani di gestione del rischio IT, (c) definizione di ruoli e organizzazione della sicurezza, (d) aggiornamento di un piano programmatico per la protezione di dati, sistemi e infrastrutture, (e) attuazione di misure di potenziamento delle capacità di gestione del rischio, in coerenza con i piani suddetti, (f) adozione delle misure previste dalle linee guida ACN, e (g) monitoraggio continuo di minacce e vulnerabilità per aggiornare le difese. Inoltre, la l. n. 90/2024, introduce la figura del "*referente per la cybersicurezza*" in ogni amministrazione e prescrive l'impiego diffuso della crittografia per proteggere i dati trattati. La normativa è stata concepita per affrontare le vulnerabilità della pubblica amministrazione, emerse anche a seguito di vari attacchi ransomware che hanno coinvolto alcuni enti locali e strutture sanitarie negli ultimi anni. Con queste misure, l'Italia si allinea (e in alcuni casi anticipa) le previsioni della direttiva NIS2 – la quale include anche le pubbliche amministrazioni di maggior dimensione tra i soggetti "essenziali" – e pone le basi per una più solida postura di cyber resilienza nel settore pubblico [6].

In sintesi, l'attuale architettura cyber italiana si fonda su un impianto normativo-istituzionale articolato: un'Agenzia nazionale dedicata (ACN) che coordina attori pubblici e privati; un Comitato Interministeriale che definisce strategie quinquennali ambiziose; un perimetro di sicurezza che vincola gli operatori critici a standard elevati; normative settoriali e trasversali (da quelle per le telecomunicazioni 5G fino al recente obbligo di certificazione cybersecurity per i servizi cloud destinati alla P.A.); costanti interventi legislativi per aggiornare obblighi e sanzioni al mutato scenario di minaccia. Questa evoluzione normativa, seppur relativamente recente, testimonia la presa di coscienza nazionale sull'importanza della cybersicurezza come fattore abilitante della trasformazione digitale in sicurezza, e, in senso lato, come requisito di sicurezza nazionale.

[6] S. ELIA, *Cybersicurezza e Pubblica Amministrazione: Strategia nazionale 2022-2026*, UniD Professional Blog, 17 novembre 2023 (https://www.unidprofessional.com/cybersicurezza); L. MARTINO, *op. cit*.

3. Governance e politiche europee di cybersecurity: attori e quadro normativo UE

A livello dell'Unione Europea, la cybersecurity è emersa progressivamente come una priorità strategica, soprattutto nel corso dell'ultimo quinquennio. Tradizionalmente, la sicurezza cibernetica rientra nelle competenze degli Stati membri (essendo connessa anche alla sicurezza nazionale), ma l'interdipendenza digitale ha spinto l'UE ad adottare un approccio sempre più integrato. Oggi possiamo parlare di un vero ecosistema normativo e istituzionale europeo della cybersecurity, composto da numerosi atti legislativi, policy e soggetti dedicati. Si stima che negli ultimi decenni siano stati emanati almeno 154 atti tra normative vincolanti e policy UE attinenti alla sicurezza cyber, mentre si possono individuare 26 attori chiave nell'architettura istituzionale dell'Unione in tale ambito. Ciò include istituzioni UE (Commissione europea, Consiglio dei ministri UE e Parlamento europeo in primis), agenzie specializzate, organismi di cooperazione tra Stati membri e altre entità [7].

Dal punto di vista istituzionale, un ruolo centrale è svolto dall'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). Creata nel 2004 come European Network and Information Security Agency, e potenziata dal *Cybersecurity Act* del 2019, ENISA funge da hub di competenze, supporto tecnico e coordinamento, assistendo Commissione e Stati membri nell'implementazione delle politiche cyber. Ad ENISA fanno capo, tra l'altro, la gestione dei programmi europei di certificazione di sicurezza informatica (introdotti proprio dal *Cybersecurity Act* del 2019) e il sostegno ai meccanismi di cooperazione come il Gruppo di Cooperazione NIS e la Rete dei CSIRT europei. Questi ultimi organismi, istituiti dalla prima direttiva NIS del 2016 e confermati dalla successiva direttiva NIS2, riuniscono periodicamente le autorità nazionali e i CERT/CSIRT dei vari paesi per condividere informazioni e *best practices* e per coordinare la gestione di incidenti su scala UE. Sul piano operativo, esiste inoltre il CERT-EU, il team di pronto intervento informatico per le istituzioni UE, recentemente inquadrato in un regolamento dedicato, il Reg. 2023/2033, il quale stabilisce misure di cybersecurity per tutte le istituzioni, organi e agenzie UE. Un altro attore emergente è il neocostituito Centro Europeo di Competenza per la Cybersecurity (ECCC) con sede a Bucarest, che insieme alla rete dei centri nazionali di coordinamento intende favorire la ricerca, l'innovazione e l'industrializzazione nel settore cyber, allocando fondi europei (programmi Digital Europe e Horizon Europe) per lo sviluppo di capacità cyber nei paesi

[7] Per un'esaustiva analisi in chiave giuridica, si rimanda al contributo di F. CASOLARI-F. FERRI-S. VILLANI, *La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea*, in questo volume.

membri. Sul piano politico-strategico, infine, va menzionato l'Alto Rappresentante dell'UE e il Servizio Europeo per l'Azione Esterna (EEAS), che guidano l'elaborazione della Strategia di Cyber Difesa dell'UE (2022) e l'attuazione del cosiddetto Cyber Diplomacy Toolbox per rispondere a livello europeo ad attacchi informatici ostili provenienti dall'esterno (inclusa la facoltà di imporre sanzioni contro attori malevoli) [8].

Passando al quadro normativo europeo, l'UE ha via via prodotto un corpus di norme sia orizzontali sia verticali, allo scopo di innalzare il livello comune di sicurezza informatica e di ridurre le disparità tra Stati membri. Un punto di svolta iniziale è stata la prima direttiva NIS (2016/1148/UE), che ha introdotto obblighi minimi di sicurezza e notifica per gli operatori di servizi essenziali (OES) e per alcuni fornitori di servizi digitali, creando al contempo i citati meccanismi di cooperazione (CSIRT network, Cooperation Group) e designando autorità nazionali competenti. Nel 2023, riconoscendo la necessità di ampliare e aggiornare questo quadro, è stata adottata la direttiva NIS2 (Direttiva (UE) 2022/2555) a sostituzione della precedente. La NIS2 estende notevolmente il proprio campo di applicazione a oltre 15 settori, includendo nuovi ambiti come la pubblica amministrazione, l'industria manifatturiera critica, la gestione delle acque reflue e dei rifiuti, e il settore agroalimentare. In particolare, la direttiva NIS2 stabilisce requisiti più dettagliati in materia di misure di sicurezza, riduce i tempi per la notifica degli incidenti significativi (notifica iniziale entro 24 ore), introduce sanzioni amministrative fino a 10 milioni di euro o il 2% del fatturato e rafforza le strutture di coordinamento a livello UE. La NIS2, elevando l'asticella per tutti, mira a colmare le lacune emerse con la direttiva NIS del 2016 e a tenere il passo con un panorama di minacce molto accresciuto. Uno degli obiettivi è anche coinvolgere maggiormente l'intera filiera, comprese le PMI fornitrici di servizi o prodotti ICT agli operatori critici, promuovendo una cultura di sicurezza lungo tutta la catena del valore.

Accanto alla NIS2, l'UE, negli ultimi anni, ha varato o proposto numerosi altri strumenti normativi in materia cyber, in linea con un approccio "tutto olistico" alla resilienza digitale. Tra i principali si segnalano:

- Direttiva relativa alla resilienza dei soggetti critici (CER) – Direttiva (UE) 2022/2557, sorella della NIS2, focalizzata però sulla resilienza fisica e organizzativa di 11 settori critici, tra cui trasporti, energia, salute, acqua, infrastrutture digitali, spazio, finanziario, pubblica amministrazione. ecc.

---

[8] A. CICCHINELLI-A. MARELLA, *Governance della cybersecurity*, *op. cit.*; C. RUPP, *Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors*, Berlino, Stiftung Neue Verantwortung (Interface), 2024 (disponibile online: https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem).

- Regolamento relativo alla resilienza operativa digitale per il settore finanziario (DORA) – Regolamento (UE) 2022/2554, applicato dal gennaio 2025, che istituisce un quadro uniforme di cybersecurity per il settore finanziario (banche, assicurazioni, società di investimento, infrastrutture di mercato, fornitori ICT critici).
- Regolamento sulla cybersicurezza (CSA) – Regolamento (UE) 2019/881, già citato, che ha conferito mandato permanente ad ENISA e introdotto l'European Cybersecurity Certification Framework. In base a questo quadro, vengono progressivamente sviluppati *schemi europei di certificazione* per prodotti, servizi e processi ICT, su base volontaria, articolati su tre livelli di affidabilità (di base, sostanziale, elevato). Lo scopo è aumentare la fiducia nella sicurezza dei prodotti digitali e ridurre la frammentazione tra diversi schemi nazionali.
- Regolamento sulla cyber resilienza (CRA) – Regolamento (UE) 2024/2847. Si tratta di un atto orizzontale che introduce requisiti obbligatori di cybersecurity per i prodotti digitali immessi sul mercato europeo, hardware e software (c.d. "prodotti con elementi digitali"), lungo tutto il loro ciclo di vita [9].
- Cyber Solidarity Act – Regolamento (UE) n. 38/2025, in vigore da febbraio 2025, che mira a rafforzare la solidarietà europea nella risposta agli attacchi informatici gravi [10]. Il Cyber Solidarity Act prevede la creazione di una sorta di "scudo cibernetico europeo" attraverso il co-finanziamento UE di avanzati Security Operations Centers (SOC) distribuiti in maniera interconnessa sul territorio dell'Unione e la costituzione di una Cyber Emergency Response Reserve. Quest'ultima consiste in gruppi di intervento rapido in cybersecurity, composti da fornitori di servizi di risposta agli incidenti selezionati, attivabili in caso di attacchi su larga scala in uno Stato membro. Inoltre, il regolamento istituisce un meccanismo di valutazione *ex post* degli incidenti maggiori (*EU Incident Review Mechanism*) per trarre insegnamenti e migliorare le prassi di difesa collettiva.

---

[9] Per un'analisi del *Cyber Resilience A*ct in merito rispettivamente agli approcci regolatori, alla prospettiva degli accordi commerciali dell'Unione e come strumento di protezione dei diritti fondamentali, si vedano in questo stesso volume i contributi di P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il Cyber Resilient Act*, G. ADINOLFI-R. MAGNAGHI, *Il Cyber Resilience Act nella prospettiva degli accordi commerciali dell'Unione europea* e V. REMONDINO, *Il Cyber Resilience Act come strumento per la protezione dei valori dell'UE? Tra esigenze di sicurezza dei prodotti e tutela dei diritti fondamentali dei singoli*.

[10] S. VILLANI, *The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System*, in *European Journal of Risk Regulation*, 2025, 1, pp. 1-13.

Oltre a questi, si potrebbero citare ulteriori provvedimenti e iniziative UE, come ad esempio: la EU Cybersecurity Strategy 2020, la quale invita ad una maggiore comunicazione con visione d'insieme delle azioni UE interne ed esterne sul tema; la strategia di Cyber Defence nel quadro della Bussola Strategica della UE (2022); la normativa sugli strumenti di cybersorveglianza *dual-use* in riferimento al Reg. 2021/821, il quale disciplina l'export controllato di strumenti che potrebbero essere usati per violazioni dei diritti umani; l'EU Cybersecurity Skills Academy, varata nel 2023 per colmare il gap di competenze cyber in Europa; il Codice di condotta rafforzato sulla disinformazione (2022) nell'ambito della co-regolamentazione DSA. Questo insieme articolato di atti delinea quella che può definirsi una politica europea integrata della cybersecurity, dove l'UE – pur rispettando le competenze nazionali – fornisce regole comuni, meccanismi cooperativi e strumenti di supporto per elevare complessivamente la sicurezza del cyberspazio europeo. L'UE è così divenuta un attore imprescindibile nella definizione delle policy cyber, con un effetto anche globale (il cosiddetto "Brussels effect") quando le sue normative spingono i grandi operatori globali ad adeguarsi ovunque ai nuovi standard europei. Allo stesso tempo, la rapidità e la vastità degli interventi UE rendono complesso l'orientamento in questo ecosistema per tutti gli stakeholder coinvolti (istituzioni, imprese, società civile). Diventa quindi cruciale un coordinamento efficace tra il livello europeo e i livelli nazionali: i Paesi membri restano i primi responsabili per la gestione operativa degli incidenti sul proprio territorio, ma la cooperazione internazionale e la condivisione di capacità diventano vitali per fronteggiare minacce che non conoscono confini [11].

4. Implicazioni politico-strategiche delle policy di cybersicurezza

L'ampio corpus di politiche e normative descritto non va valutato solo dal punto di vista tecnico o giuridico, ma anche per le implicazioni strategiche più generali che comporta. La cybersecurity policy incrocia infatti temi legati alla sovranità tecnologica, alla difesa nazionale, allo sviluppo industriale, alla tutela economica e ai valori democratici. In questa sezione analizziamo alcune chiavi di lettura trasversali ponendo l'attenzione sui seguenti temi: (*i*) l'obiettivo di un'autonomia strategica europea (e nazionale) nel digitale; (*ii*) il rafforzamento della resilienza sistemica; (*iii*) le forme di cooperazione pubblico-privato incentivate; (*iv*) l'approccio verso le minacce ibride (dove gli attacchi cyber sono

[11] A. Cicchinelli-A. Marella, *Governance della cybersecurity*, cit.; C. Rupp, *op. cit*.

usati come strumenti geopolitici); (*v*) la risposta al fenomeno dell'industrializzazione degli attacchi informatici.

4.1. Autonomia strategica e sovranità digitale

Sia l'UE che l'Italia hanno inserito esplicitamente tra gli obiettivi delle rispettive strategie di cybersecurity il perseguimento di una maggiore indipendenza strategica in ambito digitale. Ciò significa poter contare, per quanto possibile, su competenze, tecnologie e capacità industriali interne (e/o comunque sotto controllo europeo) per la protezione cibernetica, riducendo la dipendenza da fornitori esterni. Nella Strategia nazionale italiana si attribuisce particolare rilevanza allo sviluppo di tecnologie digitali sicure e al sostegno a centri di ricerca ed eccellenza nazionali, in modo da garantire "un adeguato livello di autonomia strategica nel settore" cyber. Ciò è in linea con iniziative UE come il già citato Centro Europeo di Competenza per la Cybersecurity e con i finanziamenti del programma Digital Europe per progetti cyber. L'autonomia strategica, tuttavia, non implica l'autarchia tecnologica, ma piuttosto la capacità di scelta e di controllo sulle tecnologie critiche. Un esempio concreto è la questione della sicurezza delle reti 5G. Sia l'UE (grazie alla EU 5G Toolbox del 2020) che l'Italia (col d.p.c.m. n. 1/2018 sul golden power e normative successive) hanno introdotto restrizioni verso fornitori considerati ad alto rischio, mirando non solo a diversificare, ma anche a rendere "affidabile", la supply chain delle infrastrutture digitali. Il concetto di "sovranità digitale europea", promosso dalla Commissione von der Leyen, si sostanzia anche in queste misure: stabilire regole del gioco che favoriscano innovazione e competenze locali, rendendo l'Europa non solo consumatrice ma anche produttrice di sicurezza digitale. Naturalmente, il bilanciamento tra autonomia e cooperazione globale resta una sfida aperta nel dominio cyber, dove standard e interoperabilità internazionali sono cruciali. Infatti, l'UE continua la collaborazione con alleati quali NATO e ONU per definire norme di comportamento statale nel cyberspazio e per promuovere iniziative come l'Internet Governance libera e aperta. Tuttavia, l'evidente enfasi su una robusta base industriale e scientifica propria viene considerata una precondizione per la credibilità strategica: «rafforzare le capacità tecnologiche dell'UE» e «cogliere le opportunità dell'economia dei dati garantendo riservatezza e sicurezza» sono, infatti, alcuni impegni esplicitamente assunti dai leader UE (Dichiarazione di Budapest, nov. 2024) per stimolare la competitività e ridurre il divario con i concorrenti globali [12].

[12] ISTITUTO PER LA COMPETITIVITÀ (I-COM), *Competitività alla prova della cybersecurity: La sicurezza informatica in Italia e in Europa tra innovazione e regole*, rapporto Osservatorio Cibersicurezza, presentato il 18 marzo 2025); GRUPPO TIM & CYBER SECURITY FOUNDATION,

4.2. Resilienza e gestione del rischio sistemico

Il concetto di resilienza ricorre costantemente sia nei documenti strategici che nelle normative operative. In ambito cyber, resilienza significa la capacità di un sistema (azienda, infrastruttura, Paese) di assorbire e reagire a eventi avversi – attacchi, incidenti – mantenendo continuità di funzionamento e ripristinando le funzionalità essenziali in tempi rapidi. Le policy esaminate puntano a migliorare la resilienza su vari livelli. La direttiva NIS2, ad esempio, fissa requisiti che mirano a rafforzare le difese preventive ma anche la capacità di risposta e ripristino degli operatori essenziali. Analogamente, DORA impone agli attori finanziari piani di continuità operativa ICT e test severi per assicurare che servizi critici (es. pagamenti, trading) non collassino di fronte a shock cibernetici. La direttiva CER, dal canto suo, adotta un approccio *all hazards*. Per le infrastrutture fisiche vitali, vanno infatti considerati anche gli attacchi cyber come possibili cause di malfunzionamento e, pertanto, è necessario integrare contromisure non solo tecnologiche, ma anche organizzative, come esercitazioni e piani di crisi. Sul piano nazionale, iniziative come il PSNC e la l. n. 90/2024 sulla PA servono proprio a "mettere in sicurezza" gli anelli deboli che potrebbero, se compromessi, avere effetti a cascata. La resilienza richiede, inoltre, conoscenza del contesto specifico e condivisione informativa. L'ACN e il CSIRT italiano, così come ENISA e la rete dei CSIRT europei, raccolgono informazioni sulle minacce emergenti, allertano i settori specifici ed emanano indicazioni tecniche (si pensi, ad esempio, alle notifiche rapide sulle vulnerabilità software critiche come Log4Shell). In tal senso, la collaborazione pubblico-privato è un fattore abilitante se si considera che gli operatori privati gestiscono la maggioranza delle infrastrutture e dei servizi digitali e, pertanto, scambiare dati (incidenti, *threat intelligence*) e best practices con le autorità è essenziale per ottenere un quadro completo. Questo approccio olistico indica una convergenza tra resilienza digitale e resilienza "tradizionale", dal momento che proteggere una rete elettrica o un ospedale significa curarne sia la sicurezza fisica sia quella informatica in un unico piano di rischio integrato [13].

Un altro elemento strategico legato alla resilienza risiede nell'attenzione crescente verso il fattore umano e verso le competenze. Molti attacchi hanno tutt'oggi successo per via di errori umani, scarsa preparazione o mancata applicazione di misure di base. Per tale ragione, parallelamente alle regole, si sta

Cyber Security Report 2025, pubblicato 12 giugno 2025 (disponibile sul sito TIM https://www.gruppotim.it/innovation/innovation-news/Cyber-Security-Report-2025.html).

[13] C. RUPP, *op. cit.*; R. FORSI, *Cybersecurity leva di competitività: strategie per l'innovazione europea*, in *Agenda Digitale EU*, 16 giugno 2025 (https://www.agendadigitale.eu/sicurezza/cybersecurity-leva-di-competitivita-strategie-per-linnovazione-europea/).

attualmente investendo in formazione e sensibilizzazione. Iniziative quali l'Anno europeo delle competenze 2023-2024 e piani nazionali come il Capitolo dedicato del PNRR italiano sulla formazione cyber del personale PA vanno letti proprio in quest'ottica. A livello UE, inoltre, è stata lanciata una Cyber Skills Academy (2023) e ulteriori iniziative mirate ad ampliare la forza lavoro specializzata (ad esempio, Women4Cyber e, in Italia, Cybersecurity BLUE Educazione) [14]. La mancanza di professionisti ICT qualificati rappresenta, infatti, un collo di bottiglia. L'Italia, in particolare, sconta un ritardo sul capitale umano digitale, registrando la più bassa percentuale di specialisti ICT tra le grandi economie europee e solo l'8% delle imprese che adottano soluzioni di intelligenza artificiale, contro il ~20% della Germania. Ciò incide negativamente sulla capacità di innovare e introdurre misure di sicurezza avanzate. Colmare questo gap è parte integrante dell'aumento di resilienza. Ne è riprova il fatto che la Strategia nazionale italiana include numerose azioni per la crescita delle competenze cyber fin dalla formazione scolastica (si pensi all'introduzione degli Istituti Tecnici ad indirizzo cybersecurity), e che a livello politico europeo si parla di una "quinta libertà" dell'UE – la libera circolazione della conoscenza e della ricerca – per sostenere anche la competitività e la sicurezza nell'era digitale.

4.3. Cooperazione pubblico-privato e co-regolamentazione

Una caratteristica trasversale delle moderne policy cyber è l'enfasi sulla cooperazione tra attori pubblici e privati. Data la struttura di Internet e dei servizi digitali, lo Stato da solo non può "imporre" sicurezza se le aziende non collaborano; viceversa, il mercato da solo spesso non ha incentivi sufficienti a investire in cybersecurity, specie in settori a bassa marginalità, senza un quadro di regole e supporto pubblico. Si punta dunque a modelli di co-regolamentazione, in cui norme più flessibili e basate sul rischio sono applicate con il coinvolgimento attivo dei soggetti privati regolati. L'Unione Europea ha adottato questo approccio in varie normative digitali; ad esempio, il GDPR responsabilizza le aziende a valutare autonomamente i rischi legati alla violazione della privacy e ad adottare misure appropriate, imponendo *accountability* più che prescrizioni rigide. Inoltre, la direttiva NIS2 e il DORA richiedono alle imprese di predisporre attività di risk management continuo e di auto-valutare la propria postura di sicurezza, con l'idea che chi meglio conosce i propri sistemi possa anche gestire meglio i rischi. Questo approccio *risk-based* mirato – evidenziano gli esperti – consente di calibrare obblighi e controlli in base al profilo di rischio

[14] In argomento si rimanda al capitolo di A. CARBONARO-E. GNAGNARELLA, *Cybersicurezza e fattore umano: un approccio educativo inclusivo*, in questo volume.

specifico di ciascuna entità, evitando al contempo leggi troppo rigide e *one-size-fits-all* [15]. Accanto a ciò, l'UE promuove la definizione di codici di condotta volontari e partenariati industriali. Emblematico è il Codice di condotta rafforzato sulla disinformazione del 2022, in cui piattaforme online e altri attori si impegnano su base volontaria in misure anti-fake news, integrando quanto previsto dal Digital Services Act in materia di rischi sistemici. Anche nella cybersecurity, in Europa sono nate iniziative come gli Information Sharing and Analysis Centers (ISAC) settoriali, spesso su impulso delle autorità pubbliche ma gestiti dagli operatori privati, per condividere informazioni di minaccia nel proprio settore.

In Italia, la cooperazione pubblico-privato è stata riconosciuta come asse portante sia nella Strategia nazionale che nell'azione di ACN. Quest'ultima, ad esempio, ha lanciato nel 2022 il Cybersecurity Innovation Hub per mettere in rete startup e industrie cyber nazionali con le istituzioni. Dal canto suo, il settore privato italiano, tramite Confindustria, ha istituito un Osservatorio Cybersecurity e alcune produzioni annuali (Cyber Index PMI, di cui si dirà dopo) proprio in sinergia con l'ACN e il Politecnico di Milano. I vertici di Confindustria sottolineano che la sfida della sicurezza riguarda imprese, istituzioni e cittadini e richiede un approccio condiviso: da qui la necessità di investire in tecnologie sicure, accrescere le competenze e costruire un ecosistema di collaborazione pubblico-privato che consenta alle aziende, soprattutto PMI, di proteggersi efficacemente. Questo messaggio è significativo: la fiducia reciproca tra autorità pubbliche e imprese è un ingrediente essenziale affinché le norme si traducano in azioni concrete di miglioramento della sicurezza. Costruire fiducia implica trasparenza (ad esempio le aziende devono avere la certezza che condividere con ACN informazioni su un incidente non comporterà sanzioni immediate ma piuttosto supporto), condivisione di obiettivi (proteggere il tessuto produttivo è interesse comune) e meccanismi consultivi. In effetti, molte normative UE prevedono gruppi di lavoro pubblico-privati. La NIS2, ad esempio, istituisce l'European Cyber Crises Liaison Organisation Network (EU-CyCLONe) dove siedono anche rappresentanti del settore privato per gestire crisi su larga scala; il DORA contempla che fornitori ICT critici possano essere vigilati e anche sostenuti dalle autorità; il Cyber Solidarity Act prevede di finanziare fornitori privati di servizi di *incident response* per costituire la riserva europea. Questo indica dunque un cambio di paradigma che sostituisce la tradizionale logica antagonista tra regolatori contro regolati, proponendo invece una collaborazione tra partner che uniscono competenze diverse per un fine comune. Naturalmente, restano ambiti delicati – come la

[15] Sull'approccio basato sul rischio per la regolazione della cybersicurezza, si rimanda ai contributi di R. BRIGHI, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica* e P.G. CHIARA, *op. cit.*, in questo volume.

condivisione di informazioni sensibili su attacchi in corso – in cui la collaborazione tra pubblico e privato va costruita con piattaforme sicure e protocolli precisi. A tal proposito, l'Italia, con la l. n. 90/2024, ha fatto un passo in avanti anche sotto il profilo della cooperazione in emergenza. La direttiva PCM 8 agosto 2023 recepita in tale legge obbliga infatti gli enti pubblici colpiti da un attacco a garantire pieno accesso ad ACN e ai suoi esperti ai sistemi colpiti, per consentire analisi forense e reazione tempestiva. Ciò sancisce una priorità dell'interesse collettivo nella gestione delle crisi cyber, ovvero durante un grave incidente, che invita l'ente vittima a non "chiudersi" o tergiversare, ma piuttosto a collaborare attivamente con le autorità per mitigare il danno e prevenirne la diffusione. In conclusione, l'orientamento attuale delle policy enfatizza un equilibrio tra obbligatorietà e volontarietà, dove regole flessibili e accountability spingono le aziende ad agire responsabilmente. Parallelamente, le istituzioni forniscono supporto, linee guida e coordinamento, riconoscendo la centralità del settore privato nella sicurezza collettiva [16].

4.4. Minacce ibride e dimensione geopolitica

La cybersecurity non è avulsa dal contesto geopolitico, anzi, ne è divenuta una componente primaria. Si parla di minacce ibride per indicare operazioni ostili condotte da attori statuali o parastatali che combinano strumenti diversi – attacchi cibernetici, disinformazione, coercizione economica e talvolta assetti convenzionali – per colpire paesi bersaglio senza arrivare alla guerra aperta. Da alcuni anni, L'UE e la NATO hanno sviluppato apposite strategie per contrastare le minacce ibride, riconoscendo il cyberspazio come uno dei domini di conflittualità. Gli eventi recenti, in particolare la guerra in Ucraina cominciata nel 2022, hanno confermato l'uso massiccio dello strumento cyber a fini strategici. Sia prima sia durante l'invasione russa dell'Ucraina, quest'ultima ha subito attacchi informatici dirompenti, tra cui l'impiego di *malware wiper* contro ministeri e banche, e blackout mirati alle reti elettriche. Allo stesso tempo, diversi Paesi UE, tra cui Paesi Baltici e Polonia in particolare, hanno visto aumentare gli attacchi ai propri governi e infrastrutture in un contesto di tensione regionale. Anche l'Italia è stata presa di mira a partire dal 2022-2023, periodo in cui si sono moltiplicati attacchi di matrice filo-russa a siti istituzionali italiani come forma di intimidazione politica (es. attacchi DDoS al Senato e al Ministero della Difesa rivendicati da crew pro-Russia). Come evidenziato da report di agenzie e organizzazioni del settore, negli ultimi anni il numero e la pericolosità delle

[16] ISTITUTO PER LA COMPETITIVITÀ (I-COM), *Competitività alla prova della cybersecurity: La sicurezza informatica in Italia e in Europa tra innovazione e regole. Rapporto Osservatorio Cibersicurezza*, presentato il 18 marzo 2025); CONFINDUSTRIA & GRUPPO GENERALI, *op. cit*.

minacce informatiche sono aumentati in modo costante, un fenomeno ulteriormente acuito dal conflitto tra Russia e Ucraina [17]. Questo ha indotto l'UE a rafforzare la cooperazione in materia di cyber difesa (ad esempio con l'EU Cyber Rapid Response Teams, iniziativa PESCO a cui partecipa anche l'Italia) e a varare per la prima volta, nel 2020, un regime sanzionatorio cyber. Negli ultimi due anni, l'UE ha comminato sanzioni contro individui, gruppi e entità (anche russe, nordcoreane, cinesi) ritenuti responsabili di gravi attacchi come WannaCry, NotPetya e CloudHopper, tra gli altri. In parallelo, a livello NATO, il principio di difesa collettiva dell'art. 5 è stato esteso anche al cyberspazio: un *cyberattack* di ampia portata contro un alleato potrebbe essere considerato un attacco armato all'Alleanza. Ciò denota quanto questi scenari, prima relegati alla fiction, siano ora parte di pianificazioni strategiche reali [18].

Nelle politiche europee e italiane, dunque, la minaccia di attacchi sponsorizzati da Stati ostili (o da gruppi APT legati a governi) è tenuta in primaria considerazione. La stessa istituzione di ACN in Italia è motivata, tra le altre cose, dall'esigenza di avere un organismo statale focalizzato sulla difesa civile cibernetica da minacce avanzate e coordinate. Non a caso, le strategie nazionali citano le minacce ibride e la competizione geostrategica nel digitale come fattori di rischio. Ad esempio, l'introduzione nel PSNC di controlli sugli approvvigionamenti ICT (supply chain security) e dell'obbligo di notifica anticipata di acquisto di tecnologie per enti del Perimetro servono proprio a mitigare i rischi di spionaggio o sabotaggio tramite forniture compromesse (si pensi al caso Huawei/ZTE per il 5G). Anche la tutela delle reti 5G e 6G è considerata un tassello di sicurezza nazionale. Al riguardo, dal 2019 l'Italia applica rigorosamente i poteri speciali (golden power) sulle forniture di telecomunicazioni, e a livello UE si discute di misure coordinate per eliminare gradualmente fornitori ad alto rischio. Un altro esempio di minaccia ibrida è il targeting di infrastrutture critiche civili in contesto di crisi. Nel 2022 un attacco di sospetta matrice statale mandò temporaneamente fuori uso la rete satellitare Viasat in Europa proprio all'inizio delle ostilità in Ucraina, con impatto anche su utenti civili europei. Similmente, nel 2023 si è parlato poi di possibili attacchi a cavi sottomarini per le comunicazioni digitali. In tale contesto, l'UE ha reagito con iniziative come il Joint Cyber Unit (proposta Commissione 2021) per migliorare la risposta coordinata ad attacchi su larga scala e proteggere obiettivi multipli in diversi Stati. Inoltre, la dimensione ibrida ha fatto convergere ambiti prima separati, aprendo una necessaria nuova stagione di dialogo tra la cybersecurity civile e la cyber difesa militare. In Italia ciò si traduce in una collaborazione più stretta tra ACN e Ministero della Difesa – oggi dotato di un Comando per le Operazioni

[17] Si veda, tra tutti, il rapporto Clusit 2024 sulla sicurezza ICT in Italia.

[18] L. MARTINO, *op. cit.*; C. RUPP, *op. cit.*; A. CICCHINELLI-A. MARELLA, *op. cit.*

in Rete e progetti di rafforzamento cyber militare, anche grazie al PNRR – ad esempio condividendo informazioni su campagne di minaccia in corso.

Va notato inoltre che la crescente pressione geopolitica ha avuto riflessi diretti nelle statistiche di attacco al settore pubblico e infrastrutturale. Il Cyber Security Report 2025 di TIM evidenzia che, in Italia, gli attacchi informatici contro la pubblica amministrazione sono esplosi nel 2025, passando dall'1% al 42% degli attacchi totali ricevuti. Questo dato "anomalo" (storicamente il bersaglio principale erano le aziende private per lucro finanziario) indica chiaramente una motivazione geopolitica o ideologica dietro molti attacchi recenti a ministeri, comuni, aziende sanitarie e altri enti pubblici italiani. Si tratta spesso di *denial of service*, deturpamenti di siti, o furto/esfiltrazione di dati a scopo spionaggio o propaganda. Le policy nazionali hanno reagito prevedendo esercitazioni con scenari di crisi ibrida (come la "Italia Cyber Protetta" svolta nel 2022) e includendo misure specifiche nelle pianificazioni di emergenza per garantire la continuità operativa in caso di cyberattacchi. Anche le linee guida ACN per le amministrazioni (2022) raccomandano di predisporre *incident response plan* integrati con i piani di gestione crisi generali. A livello UE, con il Cyber Solidarity Act menzionato, si formalizza un principio di solidarietà cibernetica simile a quello della protezione civile: qualora uno Stato subisca un attacco di particolare entità (magari di matrice statale), potrà ricevere supporto immediato da squadre tecniche europee e attingere a fondi comuni per ripristino e compensazione dei danni. Questo rappresenta un chiaro segnale politico attraverso il quale l'UE intende scoraggiare attori ostili dimostrando che un attacco a un membro equivarrà a misurarsi con la risposta collettiva di tutti [19].

Infine, la consapevolezza delle minacce ibride ha rafforzato le sinergie tra cybersecurity e altri domini di sicurezza nazionale. Un esempio è la protezione dei processi democratici: a partire dal 2018, sia l'Italia (con il CNAIPIC) sia l'UE (con task force dedicate) hanno aumentato le difese cyber di elezioni, referendum e simili temendo ingerenze straniere via hacking o disinformazione. Anche la disinformazione online viene trattata come una minaccia ibrida, poiché pur non essendo un "attacco" in senso tecnico, ha la capacità di minare le fondamenta delle società democratiche. Il codice di condotta UE sulla disinformazione e la East StratCom Task Force (ESCTF) dell'EEAS sono alcune risposte a questo aspetto. Insomma, le policy cyber moderne escono dal perimetro strettamente tecnico e diventano parte di un approccio integrato alla sicurezza nazionale ed europea in cui IT security, intelligence, diplomazia e difesa si coordinano. L'Italia, tramite ACN e DIS, partecipa attivamente ai consessi europei su questi temi, condividendo informazioni di minaccia (come indicato anche

[19] LISA SERVIZI, *op. cit.*; S. ELIA, *Cybersicurezza e Pubblica Amministrazione: Strategia nazionale 2022-2026*, UniD Professional Blog, 17 novembre 2023 (https://www.unidprofessional.com/cybersicurezza).

dalla NIS2) e contribuendo a sviluppare una posizione comune dell'UE nel cyberspazio internazionale (ad esempio sostenendo il quadro normativo volontario dell'ONU per un comportamento responsabile degli Stati nel cyberspazio).

4.5. Industrializzazione degli attacchi e nuove sfide tecnologiche

Un tratto peculiare dell'evoluzione delle minacce cyber è la loro "industrializzazione", ovvero l'adozione da parte dei criminali informatici (e talvolta di attori statali) di modelli di business e strumenti scalabili che rendono gli attacchi più frequenti, sofisticati e ampiamente disponibili. Si pensi al fenomeno del Ransomware-as-a-Service (RaaS), caratterizzato da gruppi criminali che sviluppano malware ransomware e li "affittano" ad affiliati, fornendo kit pronti all'uso, infrastrutture di comando e controllo, nonché servizi di negoziazione con le vittime, ottenendo in cambio una quota dei profitti. Ciò ha abbassato drasticamente la barriera d'ingresso, permettendo anche ad attaccanti relativamente poco esperti di lanciare campagne ransomware ad alto impatto appoggiandosi su questo ecosistema criminale. Il risultato è un'esplosione di casi a livello globale. In questo scenario, l'Italia non è immune. Soltanto nel 2024, il numero di attacchi ransomware di rilievo documentati è aumentato, posizionando l'Italia al secondo posto in Europa per numero di attacchi subiti (146 attacchi noti nel 2024). I settori più colpiti dal ransomware in Italia sono risultati i servizi (58% dei casi) e il manifatturiero (26%), un dato coerente con l'ampia presenza di PMI in questi comparti e con l'attrattività di colpire le supply chain produttive. Le policy di cybersecurity hanno recepito l'urgenza di affrontare i ransomware sia con misure reattive, sia con iniziative preventive. Rispettivamente, questo si è tradotto, nel primo caso, incoraggiando la reportistica di incidenti (NIS2 impone la notifica anche per attacchi ransomware significativi, e la legge italiana n. 90/2024 obbliga gli enti pubblici a segnalare immediatamente attacchi anche se non ancora completamente gestiti) e, nell'altro, promuovendo le campagne di sensibilizzazione su backup e igiene informatica, la creazione di toolkit di decrittazione gratuiti e incoraggiando a non pagare i riscatti. Inoltre, la cooperazione internazionale di polizia ha già ottenuto alcuni successi contro le reti RaaS (es. gli arresti del gruppo REvil nel 2021 e la takedown di Hive nel 2023) – un ambito dove il sostegno delle policy è fondamentale per facilitare lo scambio di prove e l'armonizzazione legislativa sui reati informatici [20].

Oltre ai ransomware, l'industrializzazione degli attacchi riguarda anche i Distributed Denial of Service (DDoS): oggi esistono servizi mercenari che offrono attacchi DDoS a pagamento, amplificando il fenomeno. TIM riporta che in Italia i DDoS sono cresciuti del 36% nel 2024 rispetto all'anno precedente, con

[20] Istituto per la Competitività (I-Com), *op. cit.*; Gruppo TIM & Cyber Security Foundation, *op. cit.*; Confindustria & Gruppo Generali, *op. cit.*

una media di 18 attacchi al giorno rilevati dal SOC TIM. Di particolare preoccupazione è l'aumento di intensità, con circa il 40% di questi attacchi che superano la soglia dei 20 Gbps di traffico, rendendone quindi sempre più difficile la mitigazione. Ciò evidenzia l'espansione dei botnet (reti di computer zombie usate per generare traffico malevolo), probabilmente grazie alla crescita esponenziale di dispositivi IoT poco protetti. Le policy per contrastarli puntano su due fronti: da un lato, incentivare i provider internet e cloud a implementare misure anti-DDoS e filtraggio; dall'altro, promuovere accordi tra stati per azioni di *takedown* delle infrastrutture botnet stesse.

Un'altra dimensione è l'uso crescente di intelligenza artificiale (IA) da parte degli attaccanti. Secondo un sondaggio di CISOs citato in letteratura, nel 33% dei casi i responsabili della sicurezza percepiscono che l'impiego di strumenti di IA generativa da parte degli attori malevoli stia aumentando l'esposizione al rischio. Abbiamo visto nell'ultimo anno esempi di phishing e truffe via email molto più convincenti grazie a testi generati da AI, deepfake di voce o video usati per ingannare, nonché malware creato con l'ausilio di algoritmi generativi. Le politiche di cybersecurity dovranno dunque adattarsi a queste sfide emergenti. A tal proposito, l'AI Act (Regolamento (UE) n. 2024/1689) già classifica alcune applicazioni di IA per la cybersicurezza come ad alto rischio, richiedendo misure specifiche, mentre a livello di difesa si investe in contromisure *AI-driven* come sistemi di detection comportamentale potenziati da strumenti di machine learning. La Strategia nazionale italiana riconosce la duplice natura dell'IA, la quale «può rafforzare la sicurezza informatica ma al contempo intensificare le minacce», segnalando la necessità di un monitoraggio continuo.

Infine, non si può trascurare il dato di contesto generale. Sul punto l'Italia, come molte economie avanzate, sta digitalizzando sempre più processi e servizi, ampliando inevitabilmente la superficie d'attacco. La trasformazione digitale della PA, l'adozione del cloud computing, dell'IoT industriale, dei sistemi di telelavoro su larga scala (aumentati significativamente dopo la pandemia Covid-19) rappresentano senza dubbio progressi che però, se non accompagnati da adeguati investimenti in sicurezza, generano nuove vulnerabilità. Le statistiche rilevano che, nonostante la crescita a due cifre negli ultimi anni, la spesa in cybersecurity in Italia rimane contenuta rispetto al PIL. Infatti, l'Italia risulta ancora all'ultimo posto tra i paesi del G7 per quota di PIL destinata alla sicurezza informatica. Ciò è dovuto soprattutto al ritardo accumulato dalle imprese più piccole; il Cyber Index PMI 2024, un rapporto curato da Confindustria e Generali su oltre 1.000 PMI italiane, evidenzia che le nostre piccole e medie imprese raggiungono in media un punteggio di 52 su 100 in maturità cyber, appena un punto in più dell'anno precedente e ancora ben al di sotto della "sufficienza" (fissata convenzionalmente a 60). Solo il 15% delle PMI può considerarsi "maturo" (cioè con strategie e misure efficaci implementate), mentre il

18% è a livello "principiante" (protezione quasi nulla) e la restante maggioranza naviga tra livelli "informato" o "consapevole" ma senza capacità operative robuste. In altre parole, oltre la metà delle PMI italiane presenta ancora un livello di preparazione considerato insufficiente secondo gli indici di maturità cyber.

Tale carenza costituisce un enorme rischio sistemico, in quanto le PMI, che costituiscono l'ossatura del tessuto produttivo nazionale, sono sempre più spesso l'anello debole sfruttato dagli attori malevoli per colpire bersagli più grandi come nel caso di supply *chain attacks*. La sfida irrisolta – come titola un'analisi recente – è quindi portare questo vasto segmento di aziende a un livello di sicurezza accettabile. Le policy attuali provano a farlo sia con obblighi diretti sia con incentivi e supporto. Il PNRR italiano, ad esempio, ha stanziato contributi per la sicurezza digitale delle piccole imprese, e Confindustria supporta le aziende nell'accesso a risorse e competenze nell'intento di creare «un ecosistema più sicuro e competitivo». Nonostante tutto, la cultura della cybersecurity sta comunque lentamente prendendo piede. In molte grandi aziende italiane oggi la sicurezza IT è diventata una priorità (il 57% delle grandi organizzazioni la indica come top priority negli investimenti digitali) e figure come il CISO (*Chief Information Security Officer*) sono sempre più presenti anche in realtà medio-piccole. Tuttavia, finché la percezione del rischio cyber non sarà diffusa anche al livello del piccolo imprenditore e finché non verrà colmato il gap di investimenti – in un mercato che, pur crescendo del ~15% annuo, partiva da valori assoluti modesti – l'Italia resterà esposta. In tal senso, come ha osservato il Vice Presidente di Confindustria Angelo Camilli, «rafforzare la sicurezza digitale significa tutelare il futuro delle nostre aziende e dell'intero sistema produttivo», richiedendo uno sforzo congiunto per creare un ecosistema più sicuro e resiliente [21].

5. Confronto tra i diversi approcci: UE, italiano e casi di altri Stati membri

L'analisi effettuata evidenzia come vi sia ormai una forte convergenza tra l'approccio italiano e quello europeo sulla cybersecurity. Mentre l'Italia negli ultimi anni ha accelerato il passo, allineandosi rapidamente alle direttive UE e spesso anticipandole con misure nazionali, l'UE, dal canto suo, ha fornito un quadro comune entro cui gli Stati membri possono rafforzare le proprie difese, pur mantenendo alcune peculiarità. La creazione dell'ACN in Italia, ad esempio, ricalca modelli già esistenti in altri Paesi UE. La Francia dispone dal 2009 di un'agenzia nazionale dedicata (ANSSI) con poteri simili, mentre la Germania ha da tempo il

[21] CONFINDUSTRIA & GRUPPO GENERALI, *op. cit*.

BSI (Ufficio Federale per la Sicurezza Informatica) come autorità centrale, istituito nel 1991 e potenziato con l'IT-Sicherheitsgesetz del 2015 e sue riforme. L'Italia ha quindi recuperato terreno dotandosi di un'agenzia sul modello franco-tedesco, superando una fase in cui le competenze erano disperse tra ministeri e intelligence. Un altro parallelo è il Perimetro di sicurezza nazionale cibernetica: provvedimenti analoghi esistono in Francia ed in Germania. Parigi prevede gli OIV – Opérateurs d'Importance Vitale, soggetti critici identificati dalla Loi de Programmation Militaire 2014 e regolamentati da ANSSI con obblighi rigorosi. La legge nazionale di Berlino, invece, accanto alla NIS, identifica categorie di KRITIS – infrastrutture critiche – con certi requisiti specifici, e dal 2021 ha introdotto un elenco di aziende considerate di particolare interesse per la sicurezza, soggette a controlli su acquisizioni estere. L'Italia con il PSNC ha quindi implementato una soluzione in linea con quelle adottate da partner chiave, segno di una visione condivisa sulla necessità di tutele rafforzate per asset strategici nazionali [22].

Tuttavia, permangono differenze di natura culturale e organizzativa. La Francia si caratterizza per una consolidata tradizione di intervento statale. ANSSI esercita poteri di ispezione diretti sugli OIV e ha sviluppato un ecosistema certificativo nazionale (France Cybersecurity, qualifica SecNumCloud per i cloud provider) ancor prima del *Cybersecurity Act* europeo. La Germania, invece, ha un'impostazione più decentralizzata e basata su standard industriali. Nello specifico, il BSI, oltre ad emanare standard (BSI Grundschutz) e linee guida, collabora strettamente con le grandi aziende tedesche, pur avendo meno potere sanzionatorio diretto rispetto ad ANSSI. L'Italia, posizionandosi temporalmente dopo, ha potuto scegliere un modello ibrido. Ad ACN vengono riconosciuti poteri regolatori e sanzionatori (ad esempio sul PSNC e su NIS), ma al tempo stesso essa mira a costruire partnership con il settore privato e le università, consapevole che l'imposizione top-down da sola sia insufficiente. Un indicatore di differenza è il grado di coinvolgimento del settore industriale nello sviluppo delle policy. In Italia, soltanto recentemente attori privati (come Telecom e Leonardo) vengono coinvolti con un ruolo consultivo nelle strategie, mentre paesi come la Gran Bretagna – fuori dalla UE ma riferimento del "modello anglosassone" – hanno da anni una stretta integrazione pubblico-privato. Il NCSC UK (National Cyber Security Centre), creato nel 2016 come parte del GCHQ ma con vocazione civile, ha un programma Industry 100 in cui esperti di aziende sono distaccati presso il NCSC per lavorare fianco a fianco con gli analisti governativi, creando un'osmosi di competenze e fiducia. L'Italia si sta muovendo in questa direzione, ma sconta qualche ritardo nella fiducia reciproca, poiché storicamente le imprese italiane hanno

[22] A. Cicchinelli-A. Marella, *op. cit.*; C. Rupp, *op. cit.*; F. Decarolis-G. De Gregorio-C. Fumagalli *et al.*, *Rules That Empower: Turning EU Digital Regulation into a Catalyst for Innovation*, IEP@BU (Bocconi University Institute for European Policymaking), 2024 (disponibile su Bocconi IEP@BU: https://iep.unibocconi.eu/rules-that-empower).

spesso sottovalutato o tenuto riservati gli incidenti, mentre ora con ACN si sta cercando di instaurare un rapporto diverso.

Riguardo le PMI, la differenza maggiore risiede non tanto nelle normative, che a livello UE valgono per tutti, quanto nei livelli di consapevolezza raggiunti nei vari paesi. Sebbene i dati del Cyber Index PMI collochino l'Italia indietro, anche altri paesi come Francia e Germania presentano anch'essi un evidente dualismo che rivela grandi aziende ben protette ma filiere di subfornitori più vulnerabili. La Germania, con la sua Mittelstand (PMI manifatturiere), ha lanciato iniziative di sensibilizzazione dedicate (es. l'Alliance für Cyber Sicherheit del BSI), mentre i Länder promuovono centri di competenza locali. La Francia investe molto nella formazione regionale di esperti e offre servizi di auditing gratuiti alle PMI tramite ANSSI. Anche l'Italia sta cercando di fare altrettanto con l'ACN, la quale ha lanciato nel 2023 un servizio di scansione delle vulnerabilità aperto anche alle PMI e ha precedentemente promosso accordi con le associazioni di categoria. Va però considerato anche l'aspetto relativo alla cultura manageriale. Se il management tedesco appare più propenso a investire in sicurezza come parte integrante della qualità industriale, in Italia c'è storicamente una tendenza a considerare la sicurezza IT un costo e non un investimento, pur riconoscendo che la mentalità sta cambiando lentamente, specie dopo casi clamorosi di danni causati da attacchi cyber.

Un altro aspetto di confronto è la preparazione normativa nazionale: alcuni Stati membri avevano infatti già anticipato la NIS2 con leggi interne. Ad esempio, la Spagna aveva aggiornato la propria normativa NIS già nel 2021, includendo settori aggiuntivi, e oggi gode di un Centro Criptológico Nacional molto attivo nel pubblicare standard di sicurezza (CCN-STIC) e nell'obbligare le pubbliche amministrazioni all'uso di prodotti certificati. In questo ambito, l'Italia è all'avanguardia. Con la recente l. n. 90/2024, ha infatti compiuto un passo significativo per integrare le PA locali, una specificità che ancora manca negli ordinamenti di molti altri Paesi.

Sul fronte sanzionatorio, poi, l'Italia è stata storicamente meno incline ad applicare sanzioni severe in ambito cyber (anche per mancanza di casistica e strumenti), mentre paesi come la Francia non hanno esitato a comminare pesanti ingiunzioni a operatori critici inadempienti. Con NIS2, anche l'Italia dovrà adottare un approccio più stringente nelle ispezioni e nelle multe – specie considerando che ACN e le autorità settoriali disporranno di più poteri, aspettandosi un cambio di passo.

In sintesi, si può osservare come l'approccio europeo fornisca una cornice unificata e punti a elevare il livello medio di tutti i paesi, mantenendo però la possibilità di misure nazionali supplementari. L'approccio italiano recente è molto in sintonia con quello europeo, segno di un'integrazione piena: l'Italia contribuisce attivamente al policy making UE (basti pensare che l'attuale direttore generale di ACN, Bruno Frattasi, è stato uno dei sostenitori di un approccio condiviso in sede UE) e recepisce le norme UE, spesso con anticipo. I punti di forza italiani includono ora una governance centralizzata chiara

(ACN), una strategia nazionale completa e strumenti normativi innovativi (PSNC). I punti deboli restano la lentezza di adeguamento del tessuto PMI e una carenza di personale qualificato che richiederà tempo per essere colmata. Altri Stati membri presentano ciascuno luci e ombre: la Francia è tra le più avanzate in capacità operative (ANSSI ha un Cyber Defense Campus e compie operazioni di scoperta minacce) ma deve coordinarsi con molte agenzie (difesa, ANSSI, ANSSI ha sedi solo a Parigi); la Germania è industrialmente robusta ma ha un coordinamento federale più complesso; i paesi nordici ed est europei (es. Estonia) hanno punte di eccellenza (e cittadini molto digitalizzati e attenti alla sicurezza) ma economie più piccole. L'approccio anglosassone, tipico del Regno Unito e in parte anche degli Stati Uniti, si distingue per il ruolo proattivo dell'intelligence e per il coinvolgimento informale del settore privato nelle difese nazionali; l'UE continentale, Italia inclusa, sta cercando di assorbirne le migliori prassi pur mantenendo un contesto normativo più formalizzato [23].

Una differenza notevole consiste nel fatto che in paesi come gli USA la cybersecurity è regolata in modo settoriale e tramite standard volontari (NIST framework) più che leggi orizzontali. Ad esempio, gli Stati Uniti non dispongono di una normativa orizzontale come la direttiva NIS2, bensì di un approccio settoriale basato su leggi specifiche per ambiti quali i servizi di pubblica utilità, il comparto bancario e la sanità. L'UE (e l'Italia con essa), invece, crede nella forza di regole comuni vincolanti. Questo mira a garantire un livello minimo di sicurezza ovunque, sebbene a volte venga avvertito come potenzialmente oneroso per le imprese. Guardando al futuro, l'armonizzazione UE faciliterà anche la cooperazione intra-UE. Le aziende italiane che operano in più paesi avranno, infatti, lo stesso schema di requisiti, e in caso di incidente grave in Italia i partner europei sapranno quali standard erano applicati, semplificando la mutua assistenza.

In conclusione, l'Italia oggi dimostra un solido allineamento con le politiche europee di cybersecurity, sia grazie alla sua contribuzione a progetti strategici, come il nuovo Centro di valutazione e certificazione europea di cyber-range nell'ambito dell'EDA a Venezia, sia recependo prontamente le direttive comuni. Le differenze con altri grandi Stati UE si stanno assottigliando di pari passo con la progressiva implementazione della NIS2 e delle nuove normative. Rimangono peculiarità negli approcci organizzativi – chi più centralista, chi più federale – e nelle priorità di investimento – paesi come Francia e Germania destinano risorse ingenti da più tempo, mentre l'Italia le sta incrementando ora anche grazie ai fondi PNRR. Nonostante tutto, il quadro generale è quello di uno schieramento coeso: di fronte a minacce globali, i paesi UE, Italia compresa, riconoscono di dover agire insieme e condividere sia oneri che responsabilità per garantire un cyberspazio europeo sicuro, resiliente e aperto.

---

[23] F. DECAROLIS *et al*., *op. cit*.; A. CICCHINELLI-A. MARELLA, *op. cit*.; C. RUPP, *op. cit*.; L. MARTINO, *op. cit*.

Parte II

Cybersicurezza e protezione degli eco-sistemi cyberfisici: una visione strumentale

Capitolo 7

Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il *Cyber Resilience Act*

Pier Giorgio Chiara [*]

Abstract: Il presente capitolo intende chiarire le scelte regolatorie fondative del regolamento (UE) 2024/2847 (*Cyber Resilience Act*, CRA) relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali. Come altri atti giuridici dell'Unione europea, soprattutto con riferimento alla regolamentazione del 'digitale', il CRA combina approcci regolatori diversi, quali: i) approccio orizzontale; ii) approccio basato sul rischio; iii) approccio di sicurezza dei prodotti. In aggiunta, l'*Explanatory Memorandum* della Commissione europea alla proposta del regolamento chiarisce che il CRA contribuisce a tutelare i diritti fondamentali. Mentre la combinazione di alcuni approcci è più risalente nella tradizione del diritto armonizzato (ad es., approccio basato sul rischio e sicurezza dei prodotti), e presenta quindi profili meno problematici, l'integrazione di un approccio basato sui diritti nelle strutture tradizionali della legislazione in materia di sicurezza dei prodotti è novità recente della tecnica legislativa dell'Unione europea e pertanto merita una riflessione critica più approfondita.

Keywords: Cyber Resilience Act – Legge sulla ciberresilienza – Diritto dell'UE – Diritto della cybersicurezza – Diritti fondamentali

Sommario: 1. Introduzione. – 2. L'approccio orizzontale. – 3. L'approccio basato sul rischio. – 4. L'approccio di sicurezza dei prodotti. – 5. Il Cyber Resilience Act e la tutela dei diritti fondamentali. – 6. Conclusione.

---

[*] Ricercatore a tempo determinato di tipo a) in informatica giuridica (IUS/20), presso CIRSFID – Alma AI e Dipartimento di Scienze Giuridiche, Università di Bologna, piergiorgio.chiara2@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

Il regolamento (UE) 2024/2847 [1], vale a dire la 'legge sulla ciberresilienza' o, com'è maggiormente noto in lingua inglese, *Cyber Resilience Act* o CRA, adottato sul finire del 2024, rappresenta l'approdo di un lungo processo di politica regolatoria. Già la seconda Strategia dell'Unione in materia di cybersicurezza [2], risalente al 2017, aveva evidenziato come le minacce cibernetiche nonché i cyberattacchi a prodotti connessi (c.d. *Internet of Things*), nelle loro componenti hardware e software, fossero aumentati in misura significativa, non solo da un punto di vista quantitativo, ma anche in termini di impatto e sofisticazione [3].

Il principale risultato sul piano legislativo scaturito dalla Strategia del 2017 è stato il regolamento (UE) 2019/881 (*Cybersecurity Act*), che rinforza il ruolo dell'ENISA (Agenzia Europea per la Cybersicurezza) e soprattutto introduce un quadro di certificazione a livello europeo per la cybersicurezza. Ancorché il rafforzamento della (cyber)sicurezza delle tecnologie ICT (prodotti, servizi e processi) fosse un obiettivo del *Cybersecurity Act* [4], due elementi hanno impedito, quanto meno nel breve termine, che questo si realizzasse compiutamente. In primo luogo, la certificazione rimane strumento di diritto privato caratterizzato dalla volontarietà; in secondo luogo, il summenzionato quadro normativo non contempla requisiti obbligatori circa la cybersicurezza della totalità dei prodotti digitali.

Nel 2020 la Commissione ha adottato la terza Strategia di cybersicurezza e, nel contesto della prima area di azione (resilienza, sovranità tecnologica e leadership), annuncia la possibilità di introdurre nuove norme orizzontali volte a migliorare la cibersicurezza di tutti i prodotti connessi e servizi associati presenti nel mercato interno [5], colmando quindi una lacuna significativa nel quadro normativo.

---

[1] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (legge sulla ciberresilienza), GU L 2024/2847, 20.11.2024. Per una disamina sulla compatibilità del CRA con il diritto del commercio internazionale si veda, in questo volume, G. ADINOLFI-R. MAGNAGHI, *Il Cyber Resilience Act nella prospettiva degli accordi commerciali dell'Unione europea*.

[2] Sul termine 'cybersicurezza', si veda, in questo volume, R. BRIGHI, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica*.

[3] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017), 450 final, pp. 2-3.

[4] Considerando 65, *Cybersecurity Act*.

[5] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020), 18 final, p. 10.

Nell'arco di un anno, la Commissione ha concluso che la mancanza di requisiti obbligatori di cybersicurezza per tutti i prodotti con elementi digitali è stata la causa principale del fallimento di mercato nella fornitura di prodotti digitali con adeguati livelli di cybersicurezza [6]. Le asimmetrie informative tra i produttori e i consumatori hanno contribuito a questo fallimento di mercato, dal momento che i secondi non avevano le necessarie capacità di valutare l'adeguatezza del livello di cybersicurezza di un prodotto oppure non avevano accesso a tali informazioni. Di conseguenza, i produttori non avrebbero avuto gli incentivi necessari per offrire prodotti 'più sicuri' dal momento che i consumatori non avrebbero ricompensato il costo maggiore investito in sicurezza. Il risultato pertanto è stato un livello di investimenti nella sicurezza dei prodotti digitali sub-ottimale [7].

Investimenti sub-ottimali nella sicurezza dei prodotti rappresentano un rischio non solo per il corretto funzionamento del mercato, ma anche per i diritti fondamentali e la sicurezza degli individui. Ogni ambito e settore della nostra società è digitalizzato ed interconnesso: una vulnerabilità in un prodotto, se sfruttata dagli attori della minaccia, può comportare serie compromissioni all'infrastruttura di reti e sistemi informativi ad esso collegati, potenzialmente con drammatici effetti 'spillover' per un'intera catena di approvvigionamento [8]. Inoltre, i prodotti connessi che costituiscono la cosiddetta "Internet delle cose" (*Internet of Things*, IoT) interagiscono senza soluzione di continuità con la dimensione "fisica" in cui operano, attraverso sistemi interconnessi di sensori e attuatori. Pertanto, la sicurezza di questi prodotti non solo è strumentale alla tutela dei diritti fondamentali alla riservatezza e protezione dei dati personali, ma è anche direttamente connessa all'incolumità fisica (*safety)* [9].

Da un punto di vista giuridico, rispetto al 2017, il quadro normativo dell'Unione appariva nel 2020 ancora frammentato in relazione ai requisiti di cybersicurezza per i prodotti digitali, dal momento che le diverse iniziative legislative adottate tra la seconda e la terza Strategia hanno affrontato solo in parte i problemi identificati. Oltre al già ricordato *Cybersecurity Act*, la Commissione

---

[6] COMMISSIONE EUROPEA, *Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715 Final Study Report*, 2021, p. 69, p. 73.

[7] *Ibid*., pp. 34-37.

[8] M. VAN'T SCHIP, *The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things*, in *European Journal of Law and Technology*, 2024, vol. 15, n. 1.

[9] A. VEDDER, *Safety, security and ethics*, in A. VEDDER-J. SCHROERS-C. DUCUING-P. VALCKE (a cura di), *Security and Law*, Intersentia, Cambridge, 2020, pp. 11-26; si veda inoltre, M. DURANTE, *Safety and security in the digital age. Trust, algorithms, standards, and risks*, in D. BERKICH-M.V. D'ALFONSO (a cura di), *On the cognitive, ethical, and scientific dimensions of artificial intelligence*, Springer, Berlino, 2019, p. 372.

adottò un approccio 'verticale', intervenendo cioè su alcuni atti giuridici della legislazione sulla sicurezza dei prodotti attraverso l'inclusione di requisiti essenziali in materia di cybersicurezza [10].

La necessità di dotare l'UE di un quadro normativo unitario e coerente con precisi obblighi per gli operatori economici coinvolti nella messa a disposizione sul mercato di prodotti con elementi digitali (non solo i fabbricanti) e requisiti di cybersicurezza lungo l'intero ciclo di vita del prodotto emerge non solo dalla già ricordata terza Strategia UE in materia, ma anche dalle conclusioni del Consiglio del 2 dicembre 2020 [11] e dalla Risoluzione del Parlamento europeo del 10 giugno 2021 [12]. Così, la Presidente della Commissione europea Von der Leyen nel discorso sullo stato dell'Unione del 2021 annunciò il futuro regolamento, proposto il 15 settembre 2022. Nel novembre 2024 venne pubblicato in G.U. dell'UE il testo definitivo del regolamento.

Le scelte regolatorie alla base del CRA sono principalmente tre. Un approccio c.d. 'orizzontale', sia con riferimento all'introduzione di requisiti di cybersicurezza 'di base', che da un punto di vista dell'ambito di applicazione oggettivo (volto cioè ad includere tutti i prodotti con elementi digitali, seppure con delle eccezioni, e non invece determinate categorie merceologiche); l'approccio basato sul rischio, divenuto ormai il modello di governance standard della regolamentazione europea del digitale [13]; ed infine l'approccio di sicurezza dei prodotti, basato sul c.d. nuovo approccio, cui ora si applicano i principi del c.d. Nuovo Quadro Legislativo [14].

---

[10] È il caso del Regolamento delegato (UE) 2022/30 della Commissione del 29 ottobre 2021 che integra la direttiva 2014/53/UE del Parlamento europeo e del Consiglio per quanto riguarda l'applicazione dei requisiti essenziali di cui all'art. 3, par. 3, lett. d), e) ed f), di tale direttiva; della proposta di Regolamento relativo alle macchine (poi Regolamento (UE) 2023/1230) o della proposta di Regolamento relativo alla sicurezza generale dei prodotti (Regolamento (UE) 2023/988).

[11] CONSIGLIO DELL'UNIONE EUROPEA, *Council conclusions on the cybersecurity of connected devices*, 2020.

[12] PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 10 giugno 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale*, (2021/2568(RSP)).

[13] G. DE GREGORIO-P. DUNN, *The European risk-based approaches: connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, vol. 59, n. 2, pp. 473-500; P.G. CHIARA-F. GALLI, *Normative Considerations on Impact Assessments in EU Digital Policy*, in *MediaLaws*, 2024, no. 1, p. 105.

[14] Il Nuovo Quadro Legislativo consiste nel regolamento (CE) n. 765/2008 e la decisione n. 768/2008/CE, nonché nel regolamento (UE) 2019/ 1020 (modificato dal CRA). In breve, la legislazione in materia di sicurezza dei prodotti si limita a stabilire requisiti essenziali che i prodotti rilevanti devono rispettare per poter essere messi a disposizione sul mercato. Per dimostrare la conformità dei prodotti ai requisiti essenziali, la legislazione armonizzata prevede diverse procedure di valutazione della conformità (c.d. moduli), tra cui è prevista la possibilità per un

È opportuno un *caveat* metodologico. La combinazione di questi approcci regolatori trova nel CRA un'applicazione organica; distinguere nettamente i loro perimetri operativi nel testo del regolamento sarebbe artificioso e, comunque, di scarsa utilità nell'implementazione delle diverse disposizioni. Ciononostante, l'adozione di questa chiave interpretativa appare particolarmente utile per illustrare il funzionamento dei meccanismi ad alta complessità tecnica e giuridica del regolamento.

Anche il regolamento (UE) 2024/1689, che stabilisce regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act*, AIA), trova fondamento nei medesimi approcci regolatori, aggiungendo, tuttavia, meccanismi significativi di tutela dei diritti fondamentali (c.d. approccio basato sui diritti) [15].

A differenza dell'AIA, tra gli obiettivi del CRA non figura la protezione dei diritti fondamentali. Tuttavia, l'*Explanatory Memorandum* allegato alla proposta del CRA della Commissione chiarisce che il regolamento rafforzerebbe in una certa misura la protezione dei diritti e delle libertà fondamentali, come la privacy, la protezione dei dati personali, la libertà d'impresa e la protezione della proprietà o della dignità e integrità personale [16].

In questo contesto, il presente capitolo si propone di analizzare criticamente le scelte strutturali e gli equilibri sottesi al *Cyber Resilience Act*, evidenziando come l'interazione tra approcci regolatori eterogenei dia forma ad un impianto normativo ad alta complessità tecnico-giuridica. In particolare, l'attenzione sarà rivolta al modo in cui il CRA riesca (o meno) a coniugare la logica tradizionale della sicurezza dei prodotti e del rischio con l'emergente esigenza di integrare la tutela dei diritti fondamentali nell'ambito della regolazione tecnica. Attraverso un esame sistematico delle scelte regolatorie alla base delle disposizioni del regolamento, nonché dei documenti preparatori, del contesto normativo e degli strumenti di *soft-law* (es., orientamenti e linee-guida pubblicate da Autorità di settore) pertinenti, il contributo intende offrire strumenti interpretativi utili per comprendere la portata e le implicazioni di questo nuovo paradigma regolatorio, evidenziandone al contempo le potenzialità e le criticità.

---

fabbricante di usare standard tecnici armonizzati sviluppati dalle organizzazioni di standardizzazione europee (CEN, CENELEC ed ETSI) dietro mandato della Commissione europea al fine di garantire la specifica tecnica di un determinato set di requisiti essenziali. Per un approfondimento maggiore, si veda COMMISSIONE EUROPEA, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, (2022/C 247/01).

[15] T. EVAS, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI,* in *AIRe – Journal of AI Law and Regulation*, 2024, vol. 1, n. 1, p. 98; M. ALMADA-N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in *Common Market Law Review*, 2025, vol. 62, n. 1.

[16] EUROPEAN COMMISSION, *Explanatory Memorandum to the Cyber Resilience Act proposal*, (COM(2022) 454 final), p. 8.

2. L'approccio orizzontale

La mancanza di un quadro normativo completo dell'Unione, che stabilisca requisiti di cybersicurezza per tutti i prodotti con elementi digitali, è stata uno dei motivi che hanno portato il legislatore europeo ad adottare il CRA [17]. Infatti, le diverse iniziative legislative intraprese fino alla pubblicazione della proposta del CRA, sia a livello nazionale che dell'Unione, hanno affrontato i rischi di cybersicurezza solo in parte, tramite una legislazione settoriale, cioè per specifiche categorie di prodotto (ad es., il regolamento sui dispositivi medici). Il risultato di questo approccio regolatorio è stata la creazione di un 'mosaico legislativo', che ha aumentato l'incertezza del diritto, ha comportato oneri aggiuntivi per le imprese e, soprattutto, ha mostrato lacune sostanziali in termini di requisiti obbligatori di cybersicurezza per tutti i prodotti – e relative componenti – con elementi digitali, contribuendo pertanto ad uno stato diffuso di insicurezza [18].

L'approccio orizzontale si declina pertanto non solo in un novero di requisiti di cybersicurezza 'di base' [19], ma anche in un ambito di applicazione oggettivo trasversale rispetto alle categorie merceologiche dei prodotti con elementi digitali. Il CRA, infatti, si applica "ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete" [20].

La portata reale e l'impatto sul mercato interno di tale approccio sono chiariti dalla definizione di 'prodotto con elementi digitali', cioè "qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immessi sul mercato separatamente" [21]. A fronte della notevole estensione della nozione di prodotto contenuta nel regolamento, in linea peraltro con altri atti giuridici dell'Unione, come la direttiva (UE) 2024/2853 sulla responsabilità per danno da prodotti difettosi [22], ponendo fine ad un dibattito che tanto ha animato la letteratura soprattutto con riferimento

[17] Cons. 4, CRA.

[18] COMMISSIONE EUROPEA, *Relazione alla proposta di regolamento CRA, 2022/0272 (COD)*, COM(2022) 454 final, p. 3.

[19] L'art. 5, par. 1, CRA lascia impregiudicata infatti la possibilità per gli Stati membri di prevedere requisiti di cybersicurezza supplementari per l'acquisto o l'uso di prodotti con elementi digitali per finalità specifiche, anche nel caso in cui tali prodotti siano acquistati o utilizzati per scopi di sicurezza nazionale o di difesa.

[20] Art. 2, par. 1, CRA.

[21] Art. 3, punto 1, CRA.

[22] Art. 4, punto 1, Direttiva (UE) 2024/2853.

alle questioni inerenti alla responsabilità civile [23], è opportuno chiarire fino a che punto i requisiti e gli obblighi del CRA si applichino al software.

Il regolamento non solo ricomprende a pieno titolo il software 'incorporato', ma anche le componenti software immesse sul mercato separatamente, nonché le c.d. soluzioni di elaborazioni dati da remoto [24], vale a dire il software sviluppato dal fabbricante, o per suo conto, ai fini del trattamento o dell'archiviazione a distanza di dati la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni, come ad esempio un'applicazione mobile che richieda l'accesso a un'interfaccia per programmi applicativi [25].

Solo a queste condizioni, quindi, una soluzione di elaborazione dati da remoto rientra nell'ambito di applicazione del CRA. Ne consegue che ad un servizio cloud la cui progettazione esuli dalla responsabilità del fabbricante di un prodotto, o ad un sito web che non supporti le funzionalità di un prodotto con elementi digitali, non si applica il CRA [26]. D'altronde, gli aspetti di cybersicurezza dei modelli di servizi di cloud quali il c.d. *software-as-a-service* sono già adeguatamente coperti dalla direttiva (UE) 2022/2555 (c.d. direttiva NIS2).

Sotto altro profilo, nonostante le doglianze della comunità di riferimento, anche il software libero ed open-source rientra nell'ambito di applicazione del CRA, a patto che sia messo a disposizione sul mercato, vale a dire, fornito per essere distribuito o utilizzato nel corso di un'attività commerciale [27], in ragione

---

[23] Si veda *ex multis* G. WAGNER, *Software as a product*, in S. LOHSSE-R. SCHULZE-D. STAUDENMAYER (a cura di), *Smart products: Münster colloquia on EU law and the digital economy VI*, Nomos, 2022, pp. 157-179.

[24] DIGITALEUROPE, commentando la proposta CRA, sosteneva che il regolamento non avrebbe dovuto comprendere il 'software generico', dal momento che opera indipendentemente da uno specifico prodotto e pertanto non è adatto allo stesso trattamento legislativo; si veda DIGITALEUROPE, *Building blocks for a scalable cyber resilience act*, in https://www.digitaleurope.org/wp/wp-content/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf, 2022, pp. 7-8. *Contra*, Eurosmart, BEUC e ANEC ritenevano che l'ambito di applicazione del CRA avrebbe dovuto includere non solo il software 'non incorporato' ma anche i servizi cloud. Cfr. EUROSMART, *Cyber Resilience Act (CRA)-new cybersecurity rules for digital products and ancillary services*, 2022, pp. 8-9; ANEC, *Anec response to EC Call for evidence for an impact assessment on the cyber resilience act (CRA) initiative*, 2022, pp. 3-5; BEUC, *Cyber resilience act: cybersecurity of digital products and ancillary services-BEUC response to public consultation*, 2022, p. 7.

[25] Cons. 11; art. 3, punto 2, CRA.

[26] Cons. 12, CRA.

[27] Cons. 18, CRA. Il considerando 15 specifica che il requisito dell'attività commerciale è soddisfatto non solo dall'applicazione di un prezzo per il prodotto, ma anche dall'applicazione di un prezzo per i servizi di assistenza tecnica quando ciò non è finalizzato esclusivamente a recuperare i costi effettivi, dall'intenzione di monetizzare altri servizi, dall'imposizione, come condizione per l'utilizzo, del trattamento di dati personali per motivi diversi dal solo miglioramento

dei drammatici impatti all'intera catena di approvvigionamento a seguito di attacchi di sicurezza a componenti open-source (eg., Log4Shell, XZ Utils) [28].

La portata dell'ambito di applicazione oggettivo del CRA conosce comunque dei limiti. Alcuni prodotti con elementi digitali sono infatti esclusi in ragione del fatto che atti giuridici settoriali dell'Unione loro applicabili si occupano dei rischi di cybersicurezza e sicurezza delle informazioni assicurando il medesimo livello di protezione del CRA. È il caso dei dispositivi medici e medico-diagnostici in vitro, dei veicoli a motore, dei prodotti aeronautici certificati in conformità al regolamento (UE) 2018/1139, nonché dell'equipaggiamento marittimo a cui si applica la direttiva 2014/90/UE [29]. Inoltre, il regolamento non si applica ai pezzi di ricambio per sostituire componenti identici in prodotti con elementi digitali, a condizione che siano fabbricati secondo le stesse specifiche, e neanche ai prodotti con elementi digitali sviluppati o modificati esclusivamente per scopi di sicurezza nazionale o difesa.

Alla luce del complicato quadro che emerge, la Commissione pubblicherà orientamenti per agevolare l'attuazione del regolamento, in particolare, chiarendo fino a che punto l'ambito di applicazione del CRA si estenda al software (quindi, le soluzioni di elaborazione dati da remoto e software libero e open-source) [30].

Per quanto attiene all'ambito di applicazione soggettivo, i destinatari degli obblighi del CRA sono tutti gli operatori economici coinvolti lungo l'intera catena di valore di un prodotto con elementi digitali (fabbricanti, distributori, importatori, rappresentanti autorizzati, fornitori di servizi di logistica), ancorché con regimi di responsabilità diversi [31]. Come si vedrà nella prossima sezione, la diversa modulazione di tali obblighi è informata da un approccio basato sul diverso rischio che il singolo operatore economico gestisce con riguardo alla fabbricazione o alla messa a disposizione sul mercato del prodotto.

---

della sicurezza, della compatibilità o dell'interoperabilità del software, o dall'accettazione di donazioni che superano i costi associati alla progettazione.

[28] L. COLONNA, *The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive*, in *Computer Law & Security Review*, 2025, vol. 56, pp. 4-5; J. TRIDGELL, *Open or Closing Doors? The Influence of 'Digital Sovereignty' in the EU's Cybersecurity Strategy on Cybersecurity of Open-Source Software*, in *Computer Law & Security Review*, 2025, vol. 56.

[29] Art. 2, CRA.

[30] Art. 26, par. 2, lett. a), CRA.

[31] Gli obblighi dei fabbricanti si estendono anche all'importatore o al distributore che immetta un prodotto sul mercato con il proprio nome o marchio o effettui una modifica sostanziale del prodotto.

3. L'approccio basato sul rischio

Come altri atti giuridici dell'Unione in materia digitale, anche il CRA segue un approccio basato sul rischio [32]. Tale approccio permea ogni aspetto del regolamento, dalla classificazione dei prodotti nell'ambito di applicazione, agli obblighi, passando per le procedure di applicazione delle norme. Pertanto, come ricordato nell'Introduzione, diverse considerazioni svolte in questa sezione necessariamente intersecheranno con gli istituti tipici della legislazione armonizzata in materia di sicurezza dei prodotti, analizzati nella sezione successiva (par. 4).

Il regolamento definisce il "rischio di cybersicurezza" secondo lo schema classico della teoria di gestione del rischio [33]: il rischio si quantifica in un danno potenziale (perdita o perturbazione), causato da un incidente. Tale prodotto è dato dalla combinazione di due fattori, vale a dire la gravità del danno e la probabilità che questo si verifichi in un incidente [34]. Un rischio di cybersicurezza è invece considerato "significativo" se, in base alle sue caratteristiche tecniche, la probabilità che provochi un incidente sia *elevata* e l'impatto negativo che potrebbe cagionare *grave* (in termini di perdite materiali e immateriali) [35].

Il regolamento tutela così diversi beni giuridici dai diversi rischi di cybersicurezza che possono interessare i prodotti con elementi digitali, non limitandosi al novero classico dell'approccio in materia di sicurezza dei prodotti (par. 4), vale a dire la salute, la sicurezza o l'incolumità degli utilizzatori [36], ma includendo anche gli stessi prodotti con elementi digitali che potrebbero potenzialmente essere danneggiati, controllati o perturbati da altri prodotti [37], la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti da parte dei soggetti essenziali di cui alla direttiva NIS2, la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali (si veda par. 5), nonché altri aspetti della tutela dell'interesse pubblico largamente inteso [38]. Siffatta prospettiva ampia e 'strumentale' risulta peraltro allineata alla definizione di cybersicurezza fornita dal regolamento UE 2019/881 (*Cybersecurity Act*), quale insieme delle attività necessarie per proteggere la rete e i sistemi

[32] G. De Gregorio-P. Dunn, *The European risk-based approaches: connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, vol. 59, n. 2, pp. 473-500.

[33] Si veda *ex multis* lo standard ISO 31000 in tema di gestione del rischio: International Standardisation Organisation, *ISO 31000:2018 Risk Management – Guidelines*, 2018.

[34] Art. 3, punto 37, CRA.

[35] Art. 3, punto 38, CRA.

[36] Cons. 10, CRA.

[37] Cons. 43, CRA.

[38] Art. 57, CRA.

informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche [39].

In relazione al diverso rischio di cybersicurezza posto in essere dalle funzionalità dei prodotti, il regolamento distingue diverse categorie di prodotti con elementi digitali. Oltre ad una categoria di prodotti con elementi digitali 'standard', il CRA distingue prodotti con elementi digitali 'importanti' e 'critici'. La prima categoria include i prodotti che hanno la funzionalità principale di una delle categorie elencate nell'Allegato III: conformemente al concetto di rischio suesposto, una funzione è elencata nell'Allegato III se è essenziale per la cibersicurezza di altri prodotti, e/o se comporta un rischio significativo di avere effetti negativi su altri prodotti o sulla salute, la sicurezza o l'incolumità dei suoi utenti [40]. Questa categoria è ulteriormente divisa in due classi: la classe I ricomprende prodotti meno rischiosi (browser autonomi e incorporati; sistemi di gestione delle password; VPN; sistemi operativi; ecc.), mentre la classe II include prodotti aventi un livello maggiore di rischio (ipervisori; firewall; microprocessori e microcontrollori).

I prodotti con elementi digitali 'critici', invece, la cui funzionalità principale rientra tra le categorie elencate all'Allegato IV (dispositivi hardware con cassette di sicurezza; gateway per contatori intelligenti; carte intelligenti), sono tali in quanto la loro funzione, oltre a soddisfare i due criteri caratterizzanti i prodotti 'importanti', è in una relazione di dipendenza critica dei soggetti essenziali della direttiva NIS2 o, alternativamente, potrebbe causare gravi perturbazioni delle catene di approvvigionamento critiche in tutto il mercato interno se si verificasse un incidente o se una vulnerabilità venisse sfruttata [41]. Come si avrà modo di vedere nella prossima sezione, la ricaduta operativa di questa tassonomia è data dalle diverse procedure di valutazione di conformità che i fabbricanti devono seguire con riguardo alle diverse tipologie di prodotti.

Come nel regolamento UE 2024/1689 (AI Act), il legislatore predetermina il livello di rischiosità di un prodotto, o sistema di IA, adottando quindi una logica anticipatoria imperniata su un modello di governance *top-down* che non lascia spazio ad una rideterminazione del rischio *ex post*, diversamente dalla scelta regolatoria fatta in materia di protezione dei dati personali con un modello di governance "co-regolatoria", esemplificata soprattutto dal principio di responsabilizzazione *ex* art. 5 GDPR [42]. A differenza dell'AI Act, tuttavia, il CRA

[39] Art. 2, punto 1, *Cybersecurity Act*.

[40] Art. 7, par. 2, CRA.

[41] Art. 8, par. 2, CRA.

[42] U. PAGALLO-P. CASANOVAS-R. MADELIN, *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*, in *The Theory and Practice of Legislation*, 2019, vol. 7, n. 1.

impone a tutti i prodotti con elementi digitali rientranti nel suo ambito di applicazione il rispetto dei requisiti essenziali, mentre solo una categoria di sistemi di IA – quelli ad alto rischio – deve essere conforme ai requisiti essenziali di cui al capo 3, sezione 2, dell'AI Act.

Sotto altro profilo, l'approccio basato sul rischio del CRA è visibile nei diversi obblighi posti in capo all'ampio ventaglio di operatori economici coinvolti nell'ambito di applicazione soggettivo del regolamento (fabbricanti, distributori, importatori, rappresentanti autorizzati), a seconda del loro ruolo e della responsabilità nella catena di approvvigionamento [43].

Il primo obbligo dei fabbricanti consiste nell'effettuare una valutazione dei rischi di cybersicurezza associati al prodotto [44], il risultato della quale deve essere tenuto conto in tutte le fasi dell'intero ciclo-vita del prodotto (dalla pianificazione alla manutenzione), non solo per identificare i rischi, ma anche i requisiti essenziali relativi al prodotto (Allegato I, sezione I, si veda par. 4) pertinenti [45]. Alcuni requisiti essenziali di cybersicurezza potrebbero non essere applicabili ad un prodotto; in questo caso il fabbricante dovrebbe fornire una chiara giustificazione nella valutazione dei rischi [46]. Questo implicito 'principio di responsabilizzazione' del fabbricante non contraddice quanto detto prima in ordine alla differenza tra CRA ed AI Act: la valutazione circa la compatibilità dei requisiti essenziali del CRA con la natura di un prodotto specifico deve essere effettuata per tutti i prodotti con elementi digitali, senza distinzioni in relazione ai rischi introdotti nel mercato.

La valutazione dei rischi deve essere inclusa dal fabbricante nella documentazione tecnica, gli elementi minimi della quale sono contenuti nell'allegato VII, e messa a disposizione del pubblico. Altri obblighi di documentazione riguardano la gestione delle vulnerabilità e delle informazioni fornite da terze parti. I fabbricanti devono rispettare ulteriori obblighi nelle fasi antecedenti la messa a disposizione sul mercato: di *due diligence* per quanto riguarda l'integrazione nel prodotto con elementi digitali di componenti forniti da terze parti, di adozione delle politiche e procedure adeguate (es., politiche di divulgazione coordinata delle vulnerabilità o per assicurare la conformità dei prodotti in serie), nonché informativi (es., dati identificativi del fabbricante e del prodotto, come numero di tipo, di lotto o serie, nonché designazione di un punto di contatto unico per le comunicazioni con gli utilizzatori ed istruzioni per gli utilizzatori).

---

[43] Gli obblighi dei fabbricanti si estendono anche all'importatore o al distributore che immetta un prodotto sul mercato con il proprio nome o marchio o effettui una modifica sostanziale del prodotto.

[44] Art. 13, par. 2, CRA.

[45] Cons. 54, CRA.

[46] Cons. 55; art. 13, par. 3, CRA.

Le responsabilità dei fabbricanti non terminano una volta che il prodotto è stato immesso sul mercato. Infatti, per l'intera durata del periodo di assistenza [47], i fabbricanti garantiscono di gestire in modo efficace le vulnerabilità, come anche di rendere disponibili per almeno 10 anni dal rilascio del prodotto gli aggiornamenti di sicurezza [48].

Nel periodo di assistenza, i fabbricanti devono poi rispettare diversi obblighi di segnalazione, in particolare, delle vulnerabilità attivamente sfruttate e degli incidenti gravi che abbiano un impatto sulla sicurezza del prodotto. Incidenti e vulnerabilità vanno notificati simultaneamente al CSIRT competente e all'ENISA, nonché agli utilizzatori del prodotto con l'indicazione di qualsiasi misura correttiva che questi possono adottare per attenuare l'impatto pregiudizievole della minaccia o dell'evento [49]. Sotto altro profilo, i fabbricanti sono tenuti a segnalare eventuali vulnerabilità scoperte nei componenti (anche open-source) integrati nel prodotto ai soggetti che li producono o mantengono.

A questo si legano anche altri obblighi "cooperativi": se i fabbricanti "correggono" le vulnerabilità scoperte nei componenti, devono condividere la *patch* con il soggetto responsabile del componente. Queste misure evidenziano come il CRA operazionalizzi il principio di sicurezza della supply-chain, stabilendo regole relative alla cybersicurezza per i diversi rapporti intercorrenti tra i fornitori e i clienti lungo l'intera catena di approvvigionamento dei prodotti con elementi digitali, un aspetto che in precedenza era regolato da clausole contrattuali basate sulle migliori pratiche di sicurezza.

Sempre sul fronte cooperativo, i fabbricanti sono tenuti a collaborare con le autorità di vigilanza del mercato, fornendo, su richiesta motivata, tutte le informazioni necessarie per dimostrare la conformità del prodotto, e, se necessario, in merito a qualsiasi misura adottata per eliminare i rischi di cybersicurezza posti dal prodotto.

---

[47] Il periodo di assistenza è determinato dal fabbricante in modo da riflettere la durata di utilizzo prevista del prodotto, tenendo conto di diversi fattori quali le ragionevoli aspettative degli utilizzatori e la natura del prodotto. Tale periodo è almeno di 5 anni salvo che il fabbricante non ritenga che il prodotto sarà utilizzato per meno di 5 anni.

[48] A tutela del consumatore, il CRA prevede che gli utilizzatori possano avere accesso all'ultima versione del software in modo gratuito se il fabbricante intenda fornire aggiornamenti di sicurezza solo all'ultima versione modificata sostanzialmente.

[49] Il fabbricante presenta una notifica di preallarme di una vulnerabilità sfruttata o di un incidente grave entro 24 ore dal momento in cui ne è venuto a conoscenza; quindi, entro 72 ore dal momento della scoperta, il fabbricante dettaglia il preallarme attraverso una notifica completa; infine, il fabbricante presenta una relazione finale entro 14 giorni dalla messa a disposizione di una misura correttiva della vulnerabilità e un mese dalla trasmissione della notifica di incidente.

4. L'approccio di sicurezza dei prodotti

L'approccio di sicurezza dei prodotti, aderente a logiche di regolazione *ex ante*, mira ad assicurare che i prodotti con elementi digitali, come gli altri prodotti oggetto della legislazione armonizzata conforme al c.d. 'Nuovo Quadro Legislativo' [50], siano sicuri (e quindi meritevoli di fiducia da parte degli utilizzatori) prima che siano immessi sul mercato.

In breve, l'attuale normativa armonizzata prevede che il contenuto della legislazione si limiti ad individuare dei "requisiti essenziali" (funzionali o prestazionali) lasciando la definizione dei dettagli tecnici a norme armonizzate europee (standard tecnici) elaborate dagli organismi europei di normazione (CEN, CENELEC ed ETSI) sulla base di una richiesta di normazione da parte della Commissione. Un prodotto, per poter essere immesso sul mercato interno, deve essere conforme ai requisiti essenziali [51]. Il prodotto si presume conforme ai requisiti essenziali se il fabbricante sceglie di applicare le norme armonizzate rilevanti nella procedura di valutazione della conformità [52].

In linea con gli istituti del Nuovo Quadro Legislativo, il CRA dispone che i prodotti con elementi digitali possano essere messi a disposizione sul mercato a condizione che rispettino i requisiti essenziali di cui all'Allegato I. Nel contesto del CRA, poi, la presunzione di conformità vista poc'anzi opera anche nel caso in cui il fabbricante abbia applicato le "specifiche comuni" rilevanti stabilite in atti di esecuzione adottati dalla Commissione nel caso in cui non siano disponibili le norme armonizzate [53]. Parimenti un prodotto con elementi digitale si presume conforme ai requisiti essenziali dell'Allegato I per il quale sono stati

---

[50] Il 'Nuovo Quadro Legislativo', adottato nel luglio 2008, e basato sul 'Nuovo Approccio' del 1985, consiste nel Regolamento (UE) 765/2008, nella Decisione 768/2008, e nel Regolamento (UE) 2019/1020.

[51] Sul funzionamento della normativa di armonizzazione dell'UE si veda COMMISSIONE EUROPEA, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, 2022, 2022/C 247/01.

[52] Ancorché gli standard tecnici armonizzati rimangano strumenti di diritto privato di natura volontaria, il meccanismo della presunzione di conformità di cui godono i prodotti sviluppati in conformità alle norme armonizzate ha portato alcuni commentatori a ritenere che abbiano una natura *de facto* obbligatoria, giacché i fabbricanti si ritroverebbero senza reali alternative. Cfr. I. KAMARA, *Standardizing Personal Data Protection*, Oxford University Press, 2025, p. 76. In generale, sulla legislazione armonizzata UE si vedano *ex multis* H. HOFMANN, *European regulatory Union? The role of agencies and standards*, in P. KOUTRAKOS-J. SNELL (a cura di), *Research handbook on the EU's internal market*, Elgar Publishing, Cheltenham, 2016; E. AL MUREDEN, *La sicurezza dei prodotti e la responsabilità del produttore: Casi e materiali*, Giappichelli, Torino, 2017.

[53] Art. 27, par. 5, CRA.

rilasciati un certificato o una dichiarazione di conformità UE nell'ambito di un sistema europeo di certificazione della cybersicurezza [54].

I requisiti essenziali di cybersicurezza relativi alle proprietà dei prodotti (parte I dell'Allegato I) mettono ancora una volta in luce la complementarità tra l'approccio al rischio e gli istituti del Nuovo Quadro Legislativo. Se il primo requisito richiede che i prodotti con elementi digitali debbano essere progettati, sviluppati e prodotti in modo da *garantire un livello adeguato di cibersicurezza in base ai rischi* (enfasi mia), l'applicazione dei rimanenti 13 requisiti, di dettaglio maggiore [55], è effettuata sulla base della *valutazione dei rischi* e *ove applicabili*, testimoniando quindi un certo grado di scalabilità – caratteristica tipica dell'approccio al rischio [56] – nel regime degli obblighi imposti ai fabbricanti. Di contro, i fabbricanti sono chiamati a soddisfare tutti gli 8 requisiti di gestione delle vulnerabilità [57] di cui alla parte II dell'Allegato I [58].

Il 3 febbraio 2025, la Commissione europea ha fatto ufficialmente richiesta agli organismi di normazione europei (CEN, CENELEC ed ETSI) di elaborare nuovi standard europei per assicurare la conformità ai requisiti essenziali del Cyber Resilience Act [59], con termini differenziati per l'adozione, a partire dal 30 agosto 2026. A supporto delle attività di standardizzazione, ENISA ha svolto due mappature al fine di identificare, nella prima, il grado di copertura offerta dagli standard di cybersicurezza esistenti più rilevanti per ogni requisito

---

[54] Art. 27, par. 8, CRA.

[55] Sono messi a disposizione sul mercato senza vulnerabilità note, e con una configurazione sicura per impostazione predefinita; garantiscono che le vulnerabilità possano essere affrontate mediante aggiornamenti di sicurezza e la protezione dall'accesso non autorizzato mediante meccanismi di controllo; proteggono la riservatezza dei dati personali o di altro tipo; ecc.

[56] Si veda nel contesto della protezione dei dati personali *ex multis* N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 2018, vol. 10, n. 1.

[57] I fabbricanti identificano e documentano le vulnerabilità e i componenti contenuti nel prodotto; affrontano e correggono tempestivamente le vulnerabilità; effettuano prove e riesami efficaci e periodici della sicurezza; condividono e divulgano pubblicamente informazioni sulle vulnerabilità risolte; ecc.

[58] Cons. 54, CRA.

[59] COMMISSIONE EUROPEA, *Commission implementing legislation of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*, C(2025) 618 final.

essenziale del CRA, evidenziando le possibili lacune da colmare [60]; nella seconda, la certificazione nel contesto del sistema europeo di certificazione della cybersicurezza basato sui criteri comuni è stata analizzata per capire fino a che punto possa essere usata per ottenere la conformità ai requisiti CRA [61].

I fabbricanti, quindi, dimostrano che i prodotti sono conformi ai requisiti essenziali attraverso la c.d. procedura di valutazione della conformità [62]. Al termine della procedura di valutazione della conformità, i fabbricanti redigono una 'dichiarazione di conformità UE che fornisca le informazioni richieste dall'Allegato V e attesti la conformità dei prodotti con elementi digitali ai requisiti essenziali di cybersicurezza *ex* Allegato I e da altri atti pertinenti della normativa di armonizzazione dell'Unione applicabili [63]. Infine, appongono la marcatura CE sul prodotto con elementi digitali in modo visibile, leggibile e indelebile [64].

A seconda del livello di rischio di cybersicurezza del prodotto con elementi digitali, il CRA impone ai fabbricanti di seguire determinate procedure di valutazione della conformità. Se, infatti, i fabbricanti hanno la piena possibilità di scegliere tra la procedura di auto-valutazione (basata sul modulo A di cui alla Decisione n. 768/2008/CE) o una svolta da terze parti (esame UE del tipo basata sul modulo B; controllo interno della produzione basata sul modulo C; garanzia della qualità totale basata sul modulo H; oppure un sistema europeo di certificazione della cybersicurezza con un livello di affidabilità almeno 'sostanziale') per i prodotti con elementi digitali "standard" [65] (vale a dire, né importanti né critici), che secondo la Commissione rappresenteranno circa il 90% dei prodotti in *scope* al regolamento [66], per i prodotti importanti e critici il CRA limita la discrezionalità dei fabbricanti.

Per quanto riguarda i prodotti importanti di classe I, il fabbricante può scegliere di applicare le norme armonizzate, le specifiche comuni o sistemi europei di certificazione della cybersicurezza con livello di affidabilità almeno "sostanziale". Se, tuttavia, questi strumenti non sono applicati (anche perché

---

[60] ENISA, *Cyber Resilience Act Requirements Standards Mapping*, 2024.

[61] ENISA, *Cyber Resilience Act implementation via EUCC and its applicable technical elements*, 2025.

[62] Decisione n. 768/2008/CE.

[63] Art. 13, par. 12; art. 28, CRA.

[64] Art. 30, CRA.

[65] Art. 32, par. 1, CRA.

[66] COMMISSIONE EUROPEA, *Directorate-General for Communications Networks, Content and Technology, Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products*, 2022, in https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products.

indisponibili), o vengono applicati solo in parte, allora il fabbricante è tenuto a scegliere una procedura da parte di terze parti, vale a dire modulo B seguito dal modulo C oppure modulo H [67].

In ragione del maggior rischio di cybersicurezza, per i prodotti importanti di classe II è esclusa l'autovalutazione del fabbricante. Infatti, il fabbricante può scegliere tra le due procedure di valutazione della conformità da parte di terzi viste sopra o, ancora, un sistema europeo di certificazione della cybersicurezza con livello di affidabilità almeno "sostanziale"[68].

Eccezionalmente, i fabbricanti di prodotti con elementi digitali "importanti", che si qualifichino come software libero e open source, possono scegliere tra le procedure disponibili ai fabbricanti dei prodotti "standard"[69].

Similmente, nel caso di prodotti con elementi digitali critici, il fabbricante deve applicare i rilevanti sistemi di certificazione della cybersicurezza se richiesto, per quella categoria di prodotto critico, da uno specifico atto delegato adottato dalla Commissione a norma dell'art. 8; in mancanza di siffatto atto di implementazione, il fabbricante può scegliere una delle procedure applicabili ai prodotti importanti di classe II [70].

Infine, il capo IV del regolamento definisce le regole relative agli organismi di valutazione della conformità. In linea con il Nuovo Quadro Legislativo, gli Stati membri designano un'autorità di notifica responsabile di istituire ed eseguire le procedure necessarie per la valutazione, la notifica degli organismi di valutazione della conformità e il monitoraggio degli stessi.

5. Il Cyber Resilience Act e la tutela dei diritti fondamentali

Nella fase di presentazione della proposta legislativa, la Commissione europea ha evidenziato come tale intervento normativo orizzontale avrebbe migliorato la tutela dei diritti e delle libertà fondamentali, come la protezione della vita privata e dei dati personali, la libertà d'impresa e la protezione della proprietà o la dignità e l'integrità della persona [71]. In particolare, aumentando il livello di cybersicurezza e resilienza dei prodotti con elementi digitali,

[67] Art. 32, par. 2, CRA.

[68] Art. 32, par. 3, CRA.

[69] Art. 32, par. 5, CRA.

[70] Art. 32, par. 4, CRA.

[71] COMMISSIONE EUROPEA, *Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020*, COM(2022) 454 final, p. 9.

il numero e la gravità degli incidenti si sarebbero ridotti, con impatti positivi per la sicurezza dei dati personali trattati dai prodotti nell'ambito di applicazione del CRA.

Una visione strumentale della cybersicurezza alla protezione dei dati personali, peraltro, è stata da sempre sostenuta dal Garante europeo della protezione dei dati personali [72] e dal Comitato europeo per la protezione dei dati personali [73], nonché dalle corti europee [74] e nazionali [75], che hanno progressivamente contribuito al radicamento della cybersicurezza nel quadro costituzionale dell'Unione con riguardo alla protezione dei diritti fondamentali [76]. Ad esempio, la crittografia è riconosciuta come una delle principali misure tecniche di cybersicurezza non solo dal CRA [77], ma anche dal GDPR [78] e dalla direttiva NIS2 [79]. Con particolare riferimento alla crittografia end-to-end, la Corte EDU ha esplicitamente riconosciuto il ruolo cruciale giocato da questa tecnologia nella tutela del diritto alla riservatezza e alla libertà di espressione, ritenendo che obblighi statutari di fornire alle autorità i mezzi per decrittare le comunicazioni cifrate end-to-end non siano proporzionati agli obiettivi legittimi perseguiti [80].

---

[72] G. BUTTARELLI, *Encryption protects security and privacy*, keynote speech all'Assemblea Nazionale francese, 21 novembre 2016; W. WIEWIÓROWSKI, *The Future of Encryption in the EU*, 2020, keynote speech del webinar ISOC 2020, p. 3; W. WIEWIÓROWSKI, *Cybersecurity and Data Protection: a necessary and powerful duo*, 28 settembre 2023.

[73] EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, 2021.

[74] Per quanto riguarda la giurisprudenza della CGUE si veda, ad esempio, la decisione in *Digital Rights Ireland c. Minister for Communications & Others* del 2014 (cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238), par. 40 e, più recentemente, *VB v Natsionalna agentsia za prihodite* del 2024 (causa C-340/21, ECLI:EU:C:2023:986), par. 55. Per quanto riguarda la Corte EDU si veda, ad esempio, la sentenza del caso *Podchasov c. Russia*, 13 febbraio 2024, n. 33696/19.

[75] Si veda la decisione della Corte Costituzionale Federale tedesca del 27 febbraio 2008, 1 BvR 370/07 (ECLI:DE:BVerfG:2008:rs20080227.1bvr037007), che riconosce un 'diritto fondamentale alla tutela della confidenzialità ed integrità dei sistemi informativi' come parte dei diritti della personalità tutelati dalla Costituzione tedesca (par. 166 ss.).

[76] L.A. BYGRAVE, *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes*, in *Computer Law & Security Review*, 2024, vol. 56, pp. 4-5.

[77] Allegato I, Parte I, punto 2), lett. e).

[78] Art. 32, par. 1, lett. a), GDPR. Cfr. L.A. BYGRAVE, *Article 32. Security of processing*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation: A Commentary (2nd edition)*, forthcoming Oxford University Press, p. 71.

[79] Art. 21, par. 2, lett. h).

[80] *Podchasov c. Russia*, cit., parr. 76-79.

Al di là della tutela dei diritti fondamentali offerta *indirettamente* dagli obblighi e dai requisiti essenziali del CRA, il testo finale del regolamento non prevede *direttamente* dei meccanismi volti ad assicurare che i prodotti con elementi digitali rispettino i diritti fondamentali, come nel caso dell'AI Act – dove l'approccio basato sui diritti informa l'intero impianto di questo atipico strumento di sicurezza dei prodotti, a partire dalla base giuridica aggiunta durante i negoziati del trilogo per regolamentare la protezione dei dati personali ai sensi dell'art. 16 TFUE [81].

Infatti, oltre a migliorare il funzionamento del mercato interno e promuovere l'adozione di un'intelligenza artificiale antropocentrica e affidabile, l'AI Act ha l'obiettivo di garantire un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta [82]. Inoltre, l'impatto negativo sui diritti fondamentali è uno dei criteri che la Commissione deve seguire nel modificare la tassonomia dei sistemi di IA ad alto rischio elencati nell'Allegato III [83]. Ancora, diversi requisiti essenziali per i sistemi di IA ad alto rischio tengono conto dei rischi per i diritti fondamentali [84] e, in aggiunta, per determinati utilizzatori, è previsto l'obbligo di condurre una valutazione d'impatto sui diritti fondamentali [85]. Infine, la Commissione può sottoporre specifici sistemi di IA ad alto rischio a una valutazione di conformità da parte di terzi, tenendo conto dell'efficacia dell'autovalutazione nel minimizzare i rischi per i diritti fondamentali [86].

Nel testo finale del CRA, invece, i pochi riferimenti espliciti ai diritti fondamentali sono rinvenibili nelle regole relative all'applicazione delle norme (*enforcement*) di cui al Capo V. L'autorità di vigilanza del mercato designata da ogni Stato membro ai fini dell'attuazione del CRA può effettuare una valutazione del prodotto con elementi digitali per quanto riguarda la sua conformità ai requisiti essenziali del CRA se ha motivi sufficienti per ritenere che tale prodotto presenti un rischio di cybersicurezza significativo, tenendo conto anche dei fattori di rischio non tecnici. Se, all'esito dell'indagine, il prodotto risulta non conforme, l'autorità chiede all'operatore economico di adottare le opportune misure correttive. Qualora l'operatore economico non dovesse collaborare,

---

[81] M. ALMADA-N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in *Common Market Law Review*, 2025, vol. 62, n. 1; cfr. T. EVAS, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI*, in *AIRe – Journal of AI Law and Regulation*, 2024, vol. 1, no. 1, p. 98.

[82] Art. 1, AI Act.

[83] Artt. 6, par. 3; 7, AI Act.

[84] Artt. 9, par. 2, lett. a); 10, par. 2, lett. f); 13, par. 3, lett. b), punto iii); 14, par. 2, AI Act.

[85] Art. 27, AI Act.

[86] Art. 43, par. 6, AI Act.

l'autorità adotta adeguate misure restrittive di natura provvisoria (es., divieto o limitazione della messa a disposizione, ritiro o richiamo): per considerarsi definitive, è necessario il decorso di 3 mesi senza obiezioni dalla Commissione e dagli altri Stati membri che hanno ricevuto la comunicazione da parte dell'autorità procedente della procedura [87].

Dopo aver effettuato l'indagine di cui sopra, l'autorità, pur rilevando la conformità del prodotto al regolamento, può tuttavia ravvisare un rischio di cybersicurezza significativo oppure, *inter alia*, un "rischio per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali"[88]. In tal caso, l'operatore economico pertinente è tenuto ad adottare le misure correttive del caso nel termine assegnato dall'autorità, che comunica le misure adottate alla Commissione e agli altri Stati membri.

È importante sottolineare il potere della Commissione di 'stimolare' la valutazione da parte delle autorità nazionali competenti se ha motivi per ritenere che un prodotto, sebbene conforme al CRA, presenti i rischi suesposti. Come nella procedura a livello dell'Unione nei confronti di prodotti non conformi di cui all'art. 56, la Commissione può effettuare la valutazione del rischio in luogo delle autorità nazionali, con il supporto dell'ENISA, a condizione che: i) vi siano circostanze che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno; ii) non siano state adottate misure efficaci da parte dell'autorità nazionale competente; iii) la Commissione abbia motivi sufficienti per ritenere che il prodotto continui a presentare rischi per tali valori fondamentali; e, iv) informi le autorità nazionali interessate [89]. La Commissione può quindi imporre una misura correttiva o restrittiva a livello dell'Unione [90].

Da un punto di vista procedurale, tuttavia, il CRA non chiarisce i criteri affinché le condizioni che permettono l'azione della Commissione possano considerarsi soddisfatte. Per quanto riguarda la prima condizione, ci si può chiedere infatti quali siano le circostanze eccezionali che giustificano l'intervento immediato della Commissione. Infatti, il considerando 112 risulta essere ben poco d'aiuto, dal momento che fa unicamente riferimento alla situazione in cui un fabbricante metta a disposizione, in diversi Stati membri, un prodotto non conforme che è utilizzato anche in settori essenziali dai soggetti NIS2 e che contenga vulnerabilità note sfruttate da soggetti malintenzionati. Nulla dice invero circa situazioni ben più problematiche relative a prodotti conformi che, al tempo stesso, presentano rischi di cybersicurezza significativi e ad altri rischi ai beni fondamentali di cui al primo paragrafo dell'art. 57 CRA.

---

[87] Art. 54, CRA.

[88] Art. 57, par. 1, CRA.

[89] Art. 57, par. 7, CRA.

[90] Art. 57, par. 8, CRA.

La seconda condizione pone altri problemi. Com'è misurata l'efficacia di una misura adottata da parte di un'autorità nazionale? Quanto tempo deve passare prima che la Commissione intervenga? Altri atti giuridici del diritto digitale UE prevedono scenari in cui, a determinate condizioni, vi è un trasferimento dei poteri di *enforcement* dalle autorità nazionali alla Commissione, si veda ad esempio il regolamento (UE) 2022/2065 (Digital Services Act). Tuttavia, l'art. 59 DSA stabilisce termini precisi per un tale trasferimento di poteri. Questa mancanza di termini lascia ancora più sorpresi se la procedura di cui all'art. 57 viene confrontata con la procedura di salvaguardia dell'Unione prevista dall'art. 55. In quel caso, la Commissione decide se le misure correttive o restrittive adottate dalle autorità nazionali siano giustificate o meno entro un termine specifico, ossia nove mesi dalla notifica da parte dell'autorità competente.

Sotto il profilo sostanziale, uno sguardo attento alla formulazione dell'art. 57 rivela come il rischio presentato dai prodotti non sia ai diritti fondamentali di per sé, come nel caso dell'AI Act [91], bensì al *rispetto degli obblighi previsti dal diritto dell'Unione o nazionale volti a tutelare i diritti fondamentali*. Se, nel primo caso, l'enfasi della valutazione risiede nel grado di violazione di uno o più diritti fondamentali, nel secondo la valutazione concerne la conformità ad una norma di secondo livello volta ad implementare i diritti fondamentali.

Ne consegue che l'esito della valutazione a cui è chiamata l'autorità procedente sembrerebbe essere binario: gli obblighi sono rispettati oppure no. Tuttavia, la linea di demarcazione tra situazioni che comportino la conformità e la non-conformità non è sempre ben definita [92]; pertanto, queste analisi *ex-ante* [93] spesso implicano valutazioni normative, a seconda dell'obbligo in questione e del contesto applicativo del prodotto sotto indagine [94]. Così, un assistente virtuale per *smart homes*, prodotto importante di classe I ai sensi dell'Allegato III CRA, che registri e analizzi ininterrottamente *by default* tutte le interazioni dell'ambiente (es., casa privata) in cui è posto, presenta *prima facie* un rischio per la conformità ai principi e obblighi del GDPR.

L'interazione tra CRA e GDPR aumenterebbe la tutela degli interessati dal momento che le autorità per la protezione dei dati non dispongono delle misure di *enforcement* delle autorità di vigilanza del mercato in caso di violazioni degli

---

[91] Art. 82, AI Act.

[92] G. MALGIERI-C. SANTOS, *Assessing the (severity of) impacts on fundamental rights*, in *Computer Law & Security Review*, 2025, vol. 56, p. 5. Cfr. R. GELLERT, *Understanding the Notion of Risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, vol. 34.

[93] Prima, cioè, che una violazione occorra.

[94] Si veda, *ex multis*, K. YEUNG-L.A. BYGRAVE, *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*, in *Regulation & Governance*, 2022, vol. 16, p. 146.

obblighi del GDPR, sebbene alcune misure restrittive, come la limitazione definitiva del trattamento *ex* art. 58(2)(f) GDPR, possano avere effetti simili a quelle previste dal CRA (es., divieto di messa a disposizione sul mercato). Nonostante ciò, le autorità di vigilanza del mercato non sembrano i soggetti pubblici più adatti a condurre valutazioni eminentemente normative basate su valori e diritti fondamentali, ambito in cui le autorità per la protezione dei dati personali hanno storicamente maggiore esperienza.

6. Conclusione

Il presente contributo si è confrontato con l'elevato livello di complessità tecnico-giuridica del regolamento europeo Cyber Resilience Act, provando a fornire una rielaborazione dei pilastri principali dello strumento attraverso le diverse scelte regolatorie effettuate dal legislatore europeo. Come detto nell'introduzione, una separazione netta e compartimentata tra i diversi approcci regolatori (orizzontale, basato sul rischio e di sicurezza dei prodotti) che vengono implementati da questo atto giuridico, ancorché utile ai fini esplicativi del saggio, rischia di esporsi a fraintendimenti. L'analisi ha infatti mostrato come in realtà questi approcci normativi trovino uno sviluppo organico e, soprattutto, compenetrato nel testo giuridico. Così, gli istituti tipici della legislazione in materia di sicurezza dei prodotti presenti nel CRA (es., requisiti essenziali, obblighi degli operatori economici, procedure di valutazione della conformità) risultano perfettamente integrati con l'approccio al rischio, che sempre di più informa la normativa europea in materia digitale. Peraltro, se, da una parte, la combinazione degli approcci orizzontale, *risk-based* e di sicurezza dei prodotti non risulta essere una novità significativa nel contesto del diritto europeo, l'ibridizzazione di questi con un approccio più marcatamente *rights-based* presenta, invero, dei rilievi di novità e, in subordine, aspetti *prima facie* problematici.

Il CRA tutela i diritti fondamentali da una duplice prospettiva, 'strumentale' e 'diretta'. Sotto il primo aspetto, una maggior resilienza dei prodotti con elementi digitali agli attacchi informatici e agli incidenti aumenta la protezione di alcuni diritti fondamentali quali la protezione dei dati personali, la riservatezza e la libertà di espressione. In secondo luogo, come visto nella sezione 5, il CRA dispiega specifici meccanismi di *enforcement* consentendo alle autorità procedenti – siano le autorità nazionali di vigilanza del mercato o, in determinate circostanze, la Commissione europea – di utilizzare importanti poteri correttivi e restrittivi nei confronti di prodotti che, seppur anche conformi al regolamento, comportano dei rischi alla conformità alla legislazione UE o nazionale che protegge i diritti fondamentali, come ad esempio il GDPR.

Capitolo 8

Il *Cyber Resilience Act* nella prospettiva degli accordi commerciali dell'Unione europea

Giovanna Adinolfi [*], Rachele Magnaghi [**]

Abstract: Il presente capitolo intende esaminare il *Cyber Resilience Act* dell'Unione europea nella prospettiva del diritto del commercio internazionale. Il punto di partenza dell'analisi risiede nel fatto che i requisiti, tanto sostanziali quanto procedurali, introdotti dai legislatori europei allo scopo di ridurre il rischio di attacchi informatici attraverso prodotti con elementi digitali, trovano applicazione anche in relazione all'immissione sul mercato dell'Unione europea di beni originari da Paesi terzi. Alla luce di ciò, appare opportuno procedere a una verifica della compatibilità del CRA con il quadro normativo multilaterale di riferimento (in particolare, l'Accordo sugli ostacoli tecnici agli scambi che fa capo all'Organizzazione mondiale del commercio), posto che la misura appare suscettibile di avere un impatto sugli scambi internazionali. Particolare attenzione è data agli obblighi di non discriminazione e necessità della misura previsti dall'Accordo TBT.

Keywords: Cyber Resilience Act – Importazioni – Accordo TBT – Non discriminazione – Necessità – Standard internazionali

---

[*] Professoressa ordinaria di diritto internazionale presso il Dipartimento di studi internazionali, giuridici e storico-politici, Università degli Studi di Milano, giovanna.adinolfi@unimi.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU. Sebbene il lavoro sia frutto di una riflessione congiunta delle autrici, sono da attribuire a Giovanna Adinolfi i paragrafi 1, 2 e 4 e a Rachele Magnaghi i paragrafi 3, 3.1, 3.2, 3.3 e 3.4.

[**] Assegnista di ricerca presso il Dipartimento di studi internazionali, giuridici e storico-politici, Università degli Studi di Milano, rachele.magnaghi@unimi.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

Il *Cyber Resilience Act* (CRA) adottato il 23 ottobre 2024 [1] si inserisce nella disciplina dell'Unione europea in materia di cybersicurezza [2]. Le sue finalità possono essere ricondotte a due specifiche esigenze. Sulla base dell'art. 114 del Trattato sul funzionamento dell'Unione europea (TFUE), i legislatori europei sono intervenuti allo scopo di superare i limiti e le lacune del quadro normativo in tema di caratteristiche tecniche dei prodotti con elementi digitali (PED) che discendeva dal combinato disposto delle legislazioni nazionali e degli atti dell'Unione europea pertinenti. Seguendo la tradizionale prospettiva del "ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato" (art. 114, par. 1 TFUE), il Regolamento dispone un'armonizzazione minima ed orizzontale definendo i requisiti essenziali che i PED devono soddisfare per essere immessi sul mercato dell'Unione. Parallelamente, il CRA non trascura il fatto che i prodotti con elementi digitali possono costituire punti di accesso ad attacchi informatici, suscettibili di avere un profondo impatto negativo sulla vita politica, economica e sociale degli Stati. Si tratta infatti sia di beni di uso comune sia di componenti essenziali per il funzionamento di organizzazioni pubbliche e private. Il CRA li definisce quindi in termini molto ampi e generali, senza far riferimento a specifiche tipologie [3], e mira a ridurre la loro vulnerabilità agli attacchi informatici migliorando le garanzie di cybersicurezza collegate al loro uso.

Questa duplice finalità (realizzazione del mercato interno nel settore rilevante e aumento dei livelli di cybersicurezza) è perseguita introducendo una disciplina sostanziale che si applica ai PED indipendentemente dalla loro origine: realizzati presso stabilimenti localizzati nel territorio dell'Unione o importati da Stati terzi, i PED possono essere commercializzati nel mercato interno solo se soddisfano i requisiti essenziali stabiliti dal CRA [4]. Da questo approccio

---

[1] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo ai requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza), GU L 2024/2847, 20.11.2024. Per una disamina, si veda, in questo volume, P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il Cyber Resilience Act*.

[2] Per una analisi delle finalità e dei contenuti normativi della strategia dell'Unione europea in materia di cybersicurezza, v. H. CARRAPICO-B. FARRAND, *Cybersecurity trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics*, in *Journal of Common Market Studies*, 2024, p. 147 e, in questo volume, F. CASOLARI, F. FERRI, S. VILLANI, *La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea*.

[3] Art. 3, parr. 1 e 2, CRA.

[4] *Ivi*, art. 4.

normativo deriva la previsione di obblighi rivolti sia a fabbricanti dell'Unione europea sia agli operatori economici coinvolti nell'immissione nel mercato interno di PED originari da paesi terzi. Quest'ultima prospettiva guida l'analisi che segue, intesa a individuare se e in quale misura il Regolamento introduca una barriera all'importazione dei beni considerati, tenendo in particolare conto degli obblighi che l'Unione ha assunto per effetto della partecipazione ad una fitta rete di trattati di liberalizzazione commerciale, *in primis* gli accordi che fanno capo all'Organizzazione mondiale del commercio (OMC).

L'esigenza di questa analisi sorge sulla base di una considerazione più generale, ovvero che le normative nazionali che fissano le caratteristiche dei beni che possono essere commercializzati nel territorio degli Stati (qui di seguito, normative tecniche) sono oggi considerate tra le principali barriere all'interscambio commerciale. Nell'ambito della loro *jurisdiction to prescribe*, gli Stati hanno da sempre mostrato una più o meno elevata propensione, nel perseguimento di finalità legittime quali la tutela dei consumatori, dell'ambiente, della sicurezza nazionale o dell'ordine pubblico, a definire i requisiti (tra cui dimensioni, composizione, etichettatura, imballaggi, processi produttivi) cui i beni devono rispondere per poter essere impiegati ed oggetto di operazioni di compravendita sul mercato nazionale. Il rilievo di queste normative è però aumentato nei decenni più recenti, in conseguenza di una serie di fattori: la ricerca scientifica e tecnologica, che ha messo in evidenza come l'utilizzo di determinati beni possa avere un impatto negativo sull'ambiente o sulla vita e la salute delle persone; le istanze provenienti dalla società civile, che sostengono la necessità che gli individui facciano scelte di consumo consapevoli; le crescenti sfide alla sicurezza nazionale, che oggi hanno non solo natura militare ma sono anche collegate al funzionamento ordinato di talune infrastrutture (quali i sistemi di trasporto, delle telecomunicazioni, energetici, sanitari ed elettorali). È proprio in questa ottica che si inserisce il *Cyber Resilience Act*, soprattutto nella sua dimensione valoriale, ove i legislatori europei hanno posto l'attenzione anche sulla difesa di taluni principi e valori fondamentali dell'Unione [5].

Al contempo, a fronte della riduzione ed eliminazione delle tradizionali barriere doganali al commercio che si è registrata a partire dal secondo dopoguerra, è emerso come le normative tecniche adottate dagli Stati possono comportare (talvolta intenzionalmente) una restrizione del commercio internazionale dei beni interessati. In generale, l'esistenza di regolamentazioni nazionali riguardo alle caratteristiche tecniche di un medesimo bene che si differenziano nei loro contenuti impedisce ai fabbricanti localizzati in uno Stato (salvo sostenere costi di produzione più elevati) di servire anche i mercati esteri. In questa prospettiva, si intende quindi analizzare se il CRA possa determinare la chiusura del mercato

[5] A tale riguardo, v. D. DIVERIO, *Le misure di armonizzazione dell'Unione europea in materia di cibersicurezza: profili istituzionali e basi giuridiche*, in *Eurojus*, 2024, p. 17 ss.

dell'Unione di prodotti con elementi digitali di origine straniera.

A questo scopo, l'analisi che segue evidenzia in primo luogo la disciplina prevista dal CRA in materia di importazione di prodotti con elementi digitali originari da Paesi terzi. Successivamente, l'attenzione sarà rivolta a verificare la compatibilità di questa normativa con gli obblighi internazionali assunti dall'Unione europea nel quadro degli accordi multilaterali facenti capo all'Organizzazione mondiale del commercio, con particolare riguardo all'Accordo sugli ostacoli tecnici agli scambi (*Agreement on Technical Barriers to Trade*, di seguito Accordo TBT). Questo, infatti, salvaguarda il potere dei 166 Membri dell'OMC di perseguire sul piano interno interessi legittimi definendo le caratteristiche tecniche dei beni commercializzati nei rispettivi mercati. Al contempo, allo scopo di impedire che le normative tecniche siano adottate con finalità (anche) protezionistiche, l'Accordo TBT pone alcune condizioni, *in primis* quelle di non discriminazione e necessità, e sollecita gli Stati ad agire in modo concertato, superando così le possibili incoerenze tra le rispettive discipline nazionali. Secondo queste diverse prospettive sarà quindi esaminato il CRA. Alcune considerazioni finali chiuderanno il lavoro.

2. L'impatto del Regolamento sulle importazioni nell'Unione europea di PED provenienti da paesi terzi

Come già anticipato, in base al CRA anche i prodotti con elementi digitali originari da Paesi terzi possono essere messi a disposizione sul mercato dell'Unione solo se soddisfano i requisiti essenziali di cybersicurezza di cui alla parte I dell'Allegato I al Regolamento e se i produttori hanno messo in atto processi conformi alla successiva parte II [6]. L'applicazione di tale comando coinvolge tre diverse categorie di soggetti, ovvero i fabbricanti esteri, gli importatori e i rappresentanti autorizzati, cui eventualmente i fabbricanti abbiano conferito mandato ad agire per loro conto [7]. Dal momento che il fabbricante estero sfugge all'ambito di applicazione territoriale del diritto dell'Unione europea, la conformità dei PED importati ai requisiti di processo e di prodotto definiti dai legislatori europei è realizzata per effetto di prescrizioni rivolte agli importatori e ai rappresentanti autorizzati, le cui attività ricadono a tutti gli effetti nella sfera di operatività del CRA [8].

[6] Art. 6 e art. 19, par. 1, CRA.

[7] V. artt. 13-15, 18 e 19, CRA.

[8] V. la definizione di rappresentante autorizzato e importatore offerta all'art. 3, rispettivamente commi 15 e 16.

In particolare, secondo l'art. 19, par. 2 CRA agli importatori si impone di accertare che il fabbricante estero dei PED che intendono immettere nel mercato dell'Unione abbia (i) redatto una *dichiarazione di conformità* di cui all'art. 28 CRA che attesti il rispetto dei requisiti essenziali di cybersicurezza previsti dal Regolamento, (ii) eseguito o fatto eseguire una *procedura di valutazione di conformità* secondo le modalità previste dal CRA e, infine, (iii) apposto la *marcatura CE* conformemente all'art. 30. Con l'intento di facilitare l'ingresso di PED esteri, i produttori stranieri possono nominare un proprio rappresentante autorizzato nel territorio dell'Unione col mandato, tra l'altro, di eseguire le attività sottoposte all'accertamento da parte degli importatori [9].

Anche per i PED importati è pienamente efficace la tecnica di armonizzazione c.d. di normalizzazione (oltre che minima e orizzontale, come sopra indicato) [10], in base alla quale il CRA si limita a prescrivere requisiti "essenziali" di cybersicurezza e rimanda la definizione di requisiti "specifici" all'adozione di "norme comuni", ovvero a) *norme armonizzate* approvate da organismi europei di armonizzazione in base al Regolamento 1025/2012 [11], b) *specifiche comuni* approvate dalla Commissione europea secondo quanto previsto all'art. 27, parr. 2.5 CRA o, infine, c) *sistemi europei di certificazione della cybersicurezza* adottati dalla Commissione europea su proposta dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA), secondo le procedure di cui agli artt. 29 e 38 del *Cybersecurity Act* (CSA) [12].

---

[9] V. il combinato disposto di art. 13, par. 12, commi 2 e 3 e art. 18, par. 2.

[10] In generale, v. T.M. MOSCHETTA, *Il ravvicinamento delle normative nazionali per il mercato interno*, Cacucci editore, Bari, 2018.

[11] Art. 27, par. 1 e par. 6, CRA. V. Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio, GU L 316, 14.11.2012, p. 12 ss. Sulle richieste avanzate dalla Commissione europea agli organismi europei di normazione per l'adozione di norme armonizzate relative ai requisiti specifici di cybersicurezza dei PED, v. i riferimenti alla nota 60 del contributo di P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti,* cit. in questo volume.

[12] Art. 27, par. 8, CRA. V. Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), GUUE L 151, 7.6.2019, p. 15 ss. Un sistema europeo è stato adottato con il Regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024 recante modalità di applicazione del regolamento (UE) 2019/771 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cybersicurezza basata sui criteri

In base alla menzionata tecnica di "normalizzazione", le norme comuni così individuate sono prive di efficacia giuridica vincolante [13]. Non è infatti escluso che la conformità ai requisiti essenziali di cui al CRA di un prodotto con elementi digitali possa essere garantita dal possesso di caratteristiche specifiche diverse da quelle indicate nelle norme comuni, sotto piena responsabilità, per i PED originari da paesi terzi, degli importatori e, eventualmente, dei rappresentanti dei produttori stranieri. L'incentivo a conformarvisi risiede tuttavia nella presunzione di conformità ai requisiti "essenziali" obbligatori, che opera laddove la dichiarazione di conformità di cui all'art. 28 CRA richiami una delle tre categorie di norme comuni.

La tecnica della normalizzazione è abbandonata per i prodotti con elementi digitali "critici" (qui di seguito, PED critici) elencati nell'Allegato IV al Regolamento [14]. In virtù delle loro funzioni specifiche, dell'importanza che rivestono per l'attività degli operatori economici in settori da cui può dipendere il funzionamento di infrastrutture o catene di approvvigionamento critiche o, infine, degli effetti particolarmente gravi di eventuali attacchi informatici nei loro confronti, è infatti riconosciuto alla Commissione il potere di stabilire che i PED critici possano essere messi in circolazione nel mercato dell'Unione europea solo se soddisfano i requisiti di cui a un sistema europeo di certificazione della cybersicurezza approvato in base al *Cybersecurity Act* [15]. Per l'accesso al mercato dell'Unione, l'importatore deve quindi accertare (e l'eventuale rappresentante autorizzato assume la responsabilità di dichiarare) che i PED critici importati sono conformi al pertinente sistema europeo.

La disciplina contenuta nel CRA si applica ai PED importati anche con riferimento a quanto previsto per le procedure di valutazione di conformità, ovvero

---

comuni (EUCC), GU L 2024/482, 7.2.2024: in dottrina, v. R. RAMPÁŠEK-M. MESARČIK-J. ANDRAŠKO, *Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification?*, in *Computer Law & Security Review*, 2025.

[13] Questa circostanza non esclude che le norme comuni approvate da organismi europei di armonizzazione siano comunque parte del diritto dell'Unione europea, giacché costituiscono «misur[e] di attuazione necessaria e strettamente regolamentata dei requisiti essenziali definiti [da un atto di diritto derivato UE], realizzata su iniziativa e sotto la direzione nonché il controllo della Commissione»: sentenza del 27 ottobre 2016, James Elliott Construction Limited c. Irish Asphalt Limited, C-613/14, EU:C:2016:821, punto 43. Per un commento, con riferimento al CRA, v. M.R. SHAFFIQUE, *Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?*, in *Computer Law & Security Review*, 2024, p. 14.

[14] Art. 8, CRA.

[15] *Ibidem*. A tale riguardo, si segnala che l'alinea 46 del preambolo al CRA afferma che taluni PED critici rientrano nell'ambito di applicazione dell'EUCC (v. *supra* n. 12) e che, pertanto, potrebbe essere opportuno subordinarne l'introduzione e la circolazione nel mercato interno al rispetto dei requisiti specifici ivi previsti.

riguardo ai processi che devono essere messi in atto per verificare che i beni in questione rispettino i requisiti essenziali di cui all'Allegato I del CRA. In tal caso, è previsto che gli importatori debbano accertare che prodotti con elementi digitali originari da paesi terzi siano stati sottoposti a una delle procedure di valutazione della conformità individuate dal Regolamento, differenziate in base al diverso rischio di cybersicurezza collegato alle loro funzionalità. L'art. 32 distingue le procedure di controllo interno condotte dal produttore estero o da un suo rappresentante autorizzato (Allegato VIII, modulo A e modulo H); le procedure realizzate da organismi autorizzati stabiliti nel territorio dell'Unione europea in ossequio alle prescrizioni dello stesso CRA (Allegato VIII, modulo B, unitamente a una procedura di controllo interno condotta secondo il successivo modulo C); infine, le procedure realizzate in base a un sistema europeo di certificazione della cybersicurezza, ove disponibile e applicabile. Vincoli stringenti sono previsti per i c.d. PED "importanti" definiti dall'art. 7 e Allegato III CRA, per i quali, in base al diverso grado di rischio, la procedura di controllo interno è esclusa *in toto* o in parte [16]. Una disciplina ancora più restrittiva è prevista per i PED critici di cui all'Allegato IV CRA [17].

Un terzo fattore sottoposto all'accertamento dell'importatore riguarda la marcatura CE quale segno distintivo. Apposta sui PED importati dal produttore straniero o da un suo rappresentante autorizzato, la marcatura deve essere conforme ai requisiti previsti dalla normativa rilevante dell'Unione [18], oltre che dall'art. 30 CRA, pena la mancata immissione nel mercato interno.

La disciplina brevemente descritta risponde all'obiettivo principale di garantire la cybersicurezza dei PED impiegati nel territorio dell'Unione europea. In sintesi, anche se importati, questi devono soddisfare i requisiti essenziali di processo e di prodotto previsti da CRA; una presunzione di conformità opera laddove i PED rispondano alle caratteristiche tecniche previste dalle eventuali specifiche comuni elaborate dalla Commissione europea o da organismi europei di armonizzazione; per i PED critici, la Commissione europea può prescrivere la loro immissione sul mercato sia subordinata al rispetto di un sistema europeo di certificazione della cybersicurezza. Inoltre, devono essere state eseguite le procedure di valutazione di conformità ai requisiti essenziali previste dal CRA, differenziate al grado di rischio relativo di ciascun PED. Infine, sul PED deve essere apposta la marcatura CE.

---

[16] Art. 32, parr. 2 e 3, CRA.

[17] *Ivi*, art. 32, par. 4.

[18] V. Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93, in GU L 218, 13.8.2008, p. 30 ss.

I PED originari da paesi terzi che non rispondono a una o più di queste caratteristiche, pur soddisfacendo gli eventuali requisiti di cybersicurezza previsti dall'ordinamento dello Stato di origine, per quanto sofisticati e adeguati a prevenire o limitare gli effetti negativi di attacchi informatici, non possono essere importati nel territorio dell'Unione. Da questo elemento discendono i potenziali effetti restrittivi sugli scambi internazionali del CRA [19].

3. La compatibilità del *Cyber Resilience Act* con l'Accordo TBT

Alla luce delle considerazioni sin qui svolte appare necessario approfondire la compatibilità del CRA con l'Accordo TBT.

Le norme dell'OMC applicabili agli ostacoli tecnici agli scambi vanno oltre le disposizioni generali relative alle barriere non tariffarie, così come stabilite nell'Accordo generale sulle tariffe doganali e sul commercio del 1994 (*General Agreement on Tariffs and Trade* – GATT 1994) e promuovono l'armonizzazione regolamentare. Invero, le disposizioni principali dell'Accordo TBT incoraggiano i Membri dell'OMC ad armonizzare le proprie misure nazionali con gli standard elaborati dagli organismi internazionali di normazione competenti.

L'Accordo riveste un ruolo centrale poiché intende garantire che le misure tecniche, pur perseguendo obiettivi legittimi di interesse pubblico, tra cui la tutela della sicurezza nazionale, non si traducano in restrizioni arbitrarie, ingiustificate o sproporzionate agli scambi internazionali.

Il CRA, introducendo requisiti essenziali per l'immissione sul mercato europeo dei PED, mette in evidenza la tensione tra la tutela di interessi pubblici legittimi – tra i quali la sicurezza nazionale riveste un ruolo preminente nel contesto della cybersicurezza [20] – e l'osservanza dei vincoli derivanti dalla disciplina commerciale multilaterale. Sotto quest'ultimo profilo, assumono particolare rilievo il principio di non discriminazione, l'obbligo di proporzionalità delle misure rispetto agli obiettivi perseguiti e la necessità di evitare che le misure adottate si traducano in barriere al commercio più gravose del necessario. In questa prospettiva, emerge con chiarezza, come già osservato in altri

[19] In generale, sul tema v. A.H. LIM, *Trade Rules for Industry 4.0. Why the Technical Barriers to Trade Agreement Matters Even More*, in S. PENG-C-F LIN-T. STREINZ (a cura di), *Artificial Intelligence and International Economic Law. Disruption, Regulation, and Reconfiguration*, Cambridge University Press, Cambridge, 2021, p. 97.

[20] N. MISHRA, *The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance*, in *Journal of World Trade*, 2020, vol. 54, n. 4, pp. 567-590.

settori [21], la necessità di operare un bilanciamento equilibrato tra interessi economici e interessi di natura non economica.

Sebbene in dottrina il CRA abbia suscitato ampie riflessioni, soprattutto in merito alla sua opportunità e alla tutela dei diritti fondamentali [22], l'aspetto della compatibilità con il diritto del commercio internazionale sembra essere rimasto in gran parte trascurato. Tale questione merita invece attenzione, considerato che il CRA costituisce anche una misura di natura commerciale e, di conseguenza, rientra nel campo di applicazione della normativa dell'OMC.

Nonostante la letteratura abbia approfondito le interazioni tra la normativa in materia di cybersicurezza e gli accordi dell'OMC [23], esaminandone differenti prospettive, tra cui quella della neutralità tecnologica [24], ad oggi, non si riscontra un'analisi specifica riguardo al CRA.

Lo scopo della presente indagine è dunque duplice: offrire un inquadramento generale della questione e, al contempo, contribuire a colmare in parte la lacuna riscontrabile nella letteratura sul punto.

A livello metodologico, l'analisi sarà condotta principalmente alla luce della giurisprudenza dell'Organo di risoluzione delle controversie (*Dispute Settlement Body* – DSB) dell'OMC.

Benché allo stato attuale non sembri verosimile l'apertura di una controversia specificamente incentrata sul Regolamento – per ragioni di opportunità politica e sistemica – risulta comunque opportuno procedere a una verifica della sua compatibilità con il quadro normativo multilaterale di riferimento, posto che

---

[21] Cfr. J. CHAISSE-C. RODRÍGUEZ-CHIFFELLE, *WTO's legacy, roadblocks, and future in global economic regulation: an introduction*, in J. CHAISSE-C. RODRÍGUEZ-CHIFFELLE (ed.), *The Elgar Companion to the World Trade Organization*, Edward Elgar Publishing, 2023, p. 7. In materia di cambiamenti climatici, ad esempio, emerge l'anacronismo di talune disposizioni dell'OMC rispetto alla necessità di affrontare problematiche contemporanee, per le quali, al fine di contrastare efficacemente il fenomeno, può rendersi necessaria l'adozione di misure talvolta restrittive per il commercio internazionale. V. *ex multis*, S. AHMAD, *Examining the Inadequacy of the GATT's Rules-Exceptions Paradigm in the Fight Against Climate Change: The Case for a WTO Climate Waiver*, in *Penn Carey Law: Legal Scholarship Repository*, 2024.

[22] P.G. CHIARA, *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction*, in *International Cybersecurity Law Review*, 2022, vol. 2, n. 3, pp. 255-272; P.G. CHIARA, *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise*, in *European Journal of Risk Regulation*, 2025, pp. 1-16; P. ECKHARDT-A. KOTOVSKAIA, *The EU's Cybersecurity Framework: The Interplay between the Cyber Resilience Act and the NIS 2 Directive,* in *International Cybersecurity Law Review*, 2023, vol. 4, n. 2, pp. 147-164.

[23] J.P. MELTZER, *Cybersecurity, Digital Trade, and Data Flows*, Working Paper n. 132 del Global Economy and Development Brookings Institution, 2020.

[24] G. GAGLIANI, *Cybersecurity, Technological Neutrality, and International Trade Law*, in *Journal of International Economic Law*, 2020, vol. 23, n. 3, pp. 723-745.

la misura pare suscettibile di avere un impatto significativo sugli scambi commerciali.

3.1. Considerazioni preliminari sulla qualificazione del CRA ai sensi del TBT

Il primo profilo giuridico che emerge in relazione al Regolamento concerne la sua qualificazione ai sensi dell'Accordo TBT. La fase di qualificazione costituisce, infatti, un presupposto indefettibile per l'avvio di un'analisi giuridica. L'Accordo disciplina una «categoria limitata di misure» [25], distinguendo, a tal fine, tra regolamenti tecnici, standard e procedure di valutazione della conformità [26], e stabilendo prescrizioni differenziate in funzione della classificazione della misura.

Considerata la complessità e la portata del CRA, tale fase risulta particolarmente articolata. Innanzitutto, occorre fare riferimento all'Allegato 1.1 dell'Accordo TBT, che definisce il regolamento tecnico come «un documento [27] che stabilisce le caratteristiche di un prodotto o i relativi processi e metodi di produzione, comprese le disposizioni amministrative applicabili, al quale la conformità è obbligatoria. Esso può altresì comprendere, o trattare esclusivamente, terminologia, simboli, requisiti di imballaggio, marcatura o etichettatura così come si applicano a un prodotto, a un processo o a un metodo di produzione».

Stante la definizione sopra riportata, l'Organo di Appello (OdA) [28] ha elaborato un test tripartito volto a determinare se una misura possa qualificarsi come regolamento tecnico [29]. In primo luogo, il prodotto oggetto della misura deve

---

[25] *European Communities – Measures Affecting Asbestos and Products Containing Asbestos*, Organo d'Appello, 5 aprile 2001, WT/DS135/AB/R, (EC – Asbestos), par. 80.

[26] Si noti che tali tre misure sono descritte nell'Allegato 1 dell'Accordo TBT.

[27] Il termine «documento» ricomprende una vasta gamma di strumenti e si applica a diverse tipologie di misure ed è definibile come «qualcosa di scritto, inciso, ecc., che fornisce prova o informazione su qualsiasi argomento» e che possiede un contenuto normativo.

[28] Per maggiori informazioni v. P. VAN DEN BOSSCHE-W. ZDOUC (eds), *The Law and Policy of the World Trade Organization: Text, Cases, and Materials*, V ed., Cambridge University Press, Cambridge, 2022, pp. 233-244; P. VAN DEN BOSSCHE, *The Demise of the WTO Appellate Body: Lessons for Governance of International Adjudication?*, WTI Working Paper, n. 02/2021, 2021.

[29] *European Communities – Trade Description of Sardine*, Organo d'Appello, 23 ottobre 2002, WT/DS231/AB/R, (EC – Sardines), par. 176; *EC – Asbestos*, *op. cit.*, parr. 66-70; *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, Panel, 24 aprile 2012, WT/DS406/R, (US – Clove Cigarettes, Panel), parr. 7.24-7.25. Si noti che tali requisiti debbono essere soddisfatti cumulativamente, v. *European Communities – Measures Prohibiting the*

essere identificato o quantomeno identificabile. In secondo luogo, il documento applicabile al prodotto così individuato deve prescrivere caratteristiche proprie del prodotto, oppure processi e metodi di produzione ad esso riferiti. Infine, il rispetto di tali caratteristiche deve essere obbligatorio.

Riguardo alla "identificabilità" del prodotto, lo stesso non deve essere esplicitamente menzionato nel documento [30]. Invero, la nozione stessa di «caratteristica del prodotto» può fungere da criterio identificativo [31]. Quest'ultima è stata interpretata come comprensiva di «qualsiasi elemento oggettivamente definibile, qualità, attributo o altro segno distintivo di un prodotto» [32].

Il secondo requisito del test, ossia la definizione delle caratteristiche del prodotto, comporta che il documento in esame contenga disposizioni che ne determinino le proprietà specifiche. Le caratteristiche del prodotto comprendono sia elementi e qualità intrinseche del bene, sia aspetti ad esse connessi, quali i mezzi di identificazione, le modalità di presentazione e l'aspetto esteriore del prodotto [33]. L'importanza di queste caratteristiche correlate è chiarita dalla seconda frase dell'Allegato 1.1, secondo cui i regolamenti tecnici possono «comprendere o trattare esclusivamente terminologia, simboli, imballaggio, marcatura o requisiti di etichettatura» [34]. Sulla base di tale disposizione, requisiti relativi all'etichettatura o all'imballaggio sono stati ritenuti costituire regolamenti tecnici in diversi contenziosi [35].

Infine, affinché una misura possa essere qualificata come regolamento tecnico, essa deve disciplinare le caratteristiche del prodotto in «modo vincolante o cogente» [36]. In altri termini, la conformità ai requisiti deve risultare obbligatoria. A tale scopo, la presenza di sanzioni pecuniarie o penali poste a presidio del rispetto delle caratteristiche sancite dalla misura costituisce, di norma, un chiaro indicatore del carattere obbligatorio della stessa [37].

Importation and Marketing of Seal Products, Organo d'Appello, 18 giugno 2014, WT/DS400/AB/RWT/DS401/AB/R, (EC – Seal Products), parr. 5.28-5.29.

[30] *EC – Sardines*, *op. cit.*, parr. 176, 182, 183.

[31] *EC – Asbestos*, *op. cit.*, par. 70.

[32] Idem, par. 67.

[33] Idem.

[34] *EC – Seal Products*, *op. cit.*, par. 5.14. L'OdA ha precisato che gli elementi indicati in tale seconda frase «si aggiungono a, e possono essere distinti da» quelli contemplati nella prima frase dell'Allegato 1.1.

[35] Per maggiori dettagli cfr. E. SHEARGOLD, *Article 1 and Annex 1 TBT: General Provisions and Terms and Their Definitions*, in P-T. STOLL (ed.), *Commentaries on World Trade Law Online*, Brill | Nijhoff, 2022.

[36] *US – Tuna II (Mexico)*, *op. cit.*, par. 185.

[37] V. *EC – Asbestos*, *op. cit*., par. 72.

Alla luce di queste premesse, come già anticipato, il CRA prevede che i PED possano essere immessi sul mercato «soltanto se» (i) soddisfano i requisiti essenziali di cybersicurezza di cui alla parte I dell'Allegato I; e (ii) i processi predisposti dai fabbricanti per la loro produzione rispettano i requisiti stabiliti nella parte II del medesimo Allegato [38]. Inoltre, il Regolamento impone per i PED importanti (Allegato III) e i PED critici (Allegato IV) ulteriori requisiti per garantire la loro sicurezza informatica, alla luce dei maggiori rischi di vulnerabilità [39].

Il CRA stabilisce dunque le caratteristiche dei PED che gli operatori economici *devono* rispettare affinché i PED possano essere immessi sul mercato.

Ai fini dell'attestazione della conformità a tali requisiti, il Regolamento prevede l'apposizione della marcatura CE [40] accompagnata dalla dichiarazione di conformità [41], con eventuale possibilità o necessità di avvalersi di norme e sistemi europei di riferimento e quindi fruire di una presunzione di conformità [42]. Invero, per i PED critici, il ricorso al sistema europeo di certificazione della cybersicurezza – in alcune circostanze – diviene necessario ai fini dell'attestazione della conformità dei prodotti e, conseguentemente, della loro immissione sul mercato [43].

Il Regolamento prevede altresì procedure di valutazione della conformità differenziate in funzione del rischio relativo al prodotto [44] e definisce un quadro chiaro e vincolante per garantire la sicurezza dei prodotti digitali e la conformità ai requisiti essenziali, contribuendo alla protezione degli utenti e alla libera circolazione dei PED nel mercato interno dell'Unione europea.

Infine, il CRA prevede, *inter alia*, sanzioni amministrative in caso venga rilevata la non conformità ai requisiti essenziali prescritti [45].

Considerate tali principali caratteristiche del CRA e la definizione contenuta nell'Allegato 1.1 del TBT, si può dunque concludere che esso costituisce un regolamento tecnico ai sensi dell'Accordo.

Ciò comporta l'applicabilità dei principi enucleati nell'art. 2 TBT, i cui profili più rilevanti saranno esaminati nel dettaglio nelle sezioni successive.

---

[38] Art. 6, CRA.

[39] *Ivi*, artt. 7-8.

[40] *Ivi*, art. 30, v. *supra*.

[41] *Ivi*, art. 28, v. *supra*.

[42] *Ivi*, art. 27, v. *supra*.

[43] *Ivi*, art. 8, par. 1. Ai sensi dell'art. 32, par. 4 b), laddove le condizioni di cui all'art. 8 non sono soddisfatte agli operatori è garantita la possibilità di ricorrere alle procedure di conformità previste per i PED importanti di classe II.

[44] *Ivi*, art. 32.

[45] *Ivi*, art. 64.

Più nello specifico, essi includono il principio della nazione più favorita e del trattamento nazionale (art. 2.1), la prevenzione di ostacoli non necessari al commercio internazionale (art. 2.2), l'armonizzazione e il ricorso a standard internazionali (art. 2.4) e il riconoscimento dell'equivalenza (art. 2.7).

Per ragioni di completezza, va osservato che la complessità del CRA comporta l'emergere di ulteriori profili – seppur di minor rilevanza – ai sensi dell'Accordo TBT, che tuttavia, per motivi di sintesi e opportunità, non saranno approfonditi in questa sede.

L'Allegato 1.3 del TBT, definisce «procedura di valutazione della conformità» una «procedura utilizzata, direttamente o indirettamente, per determinare che i requisiti pertinenti nei regolamenti tecnici o nelle norme siano soddisfatti». Ai sensi della nota esplicativa all'Allegato 1.3, le procedure di valutazione della conformità «includono, tra l'altro, procedure di campionamento, prova e ispezione; valutazione, verifica e assicurazione della conformità; […]» [46].

Alla luce di tale definizione, appare evidente che le procedure di cui all'Allegato VIII del CRA rientrino nella categoria delle procedure di valutazione della conformità e, pertanto, soggiacciano all'applicazione degli artt. 5-9 dell'Accordo TBT. Invero, come ben sottolineato dalla giurisprudenza del DSB, un singolo provvedimento può contenere sia un regolamento tecnico sia le relative procedure di valutazione della conformità [47], situazione che appare applicabile anche al CRA.

Va tuttavia osservato che se sotto il profilo del regolamento tecnico, il CRA introduce requisiti essenziali e distinzioni in termini di obblighi basati sul livello di rischio presentato dalle categorie di PED [48], sul piano delle procedure di conformità esso si limita a richiamare i moduli già stabiliti e previsti dalla Decisione 768/2008/CE, senza introdurre modifiche di carattere sostanziale alle stesse.

Pertanto, il carattere innovativo e al contempo potenzialmente problematico del CRA, che richiede una valutazione attenta alla luce dell'Accordo TBT, si rinviene nel suo inquadramento quale regolamento tecnico, piuttosto che nelle procedure di valutazione della conformità da esso previste. Precisamente, acquisiscono particolare rilevanza i requisiti essenziali prescritti dal CRA all'Allegato I per tutti i PED. Invero, essi appaiono *prima facie* suscettibili di creare discriminazione e di configurarsi come un ostacolo tecnico agli scambi internazionali [49].

---

[46] *Russia – Measures Affecting the Importation of Railway Equipment and Parts Thereof*, Organo d'Appello, 5 marzo 2020, WT/DS499/AB/R, par. 5.210.

[47] *European Communities – Protection of Trademarks and Geographical Indications for Agricultural Products and Foodstuffs*, Panel, 20 aprile 2005, WT/DS290/R, par. 7.512.

[48] Cfr. P.G. CHIARA, *The Cyber Resilience Act*, *op. cit*.

[49] Art. 42, par. 4, CRA.

Ulteriore profilo di interesse, ai sensi del diritto OMC, risulta essere il richiamo "vincolante" al sistema EUCC previsto per i PED critici individuati con atto delegato dalla Commissione. Sebbene il richiamo al EUCC – considerato isolatamente – possa rientrare nella definizione di "standard" di cui all'Allegato 1.2 TBT [50], nell'ambito dei PED critici la loro potenziale trasformazione in prescrizioni vincolanti ne muterebbe la qualificazione in regolamento tecnico, con la conseguente applicabilità della normativa pertinente.

3.2. Conformità del CRA all'art. 2.1 del TBT

Essendo un regolamento tecnico, nell'analisi del CRA assume particolare rilievo, in primo luogo, il principio di non discriminazione sancito dall'art. 2.1 dell'Accordo TBT.

La norma, come interpretata dalla giurisprudenza dell'OMC, delinea un "test a tre livelli" che richiede di verificare se (i) la misura costituisce un regolamento tecnico; (ii) i prodotti importati e quelli nazionali siano considerati prodotti «simili»; e (iii) ai prodotti importati sia garantito un trattamento non meno favorevole rispetto ai prodotti nazionali simili [51]. In tale contesto, assume preminente rilievo il concetto di «trattamento non meno favorevole», che deve essere interpretato alla luce del contesto normativo, nonché dell'oggetto e della finalità proprie dell'Accordo TBT [52]. Quest'ultimo mira a perseguire un equilibrio tra l'obiettivo della liberalizzazione degli scambi e il diritto dei Membri dell'OMC di adottare regolamentazioni volte alla tutela di obbiettivi legittimi [53].

Come costantemente affermato dal DSB dell'OMC [54], l'interpretazione dell'art. 2.1 TBT deve essere effettuata tenendo conto del contesto sistematico offerto dallo stesso Accordo, in particolare dell'art. 2.2 e del preambolo che, nel

---

[50] Si noti che tale definizione riproduce quella di regolamento tecnico con la sola differenza della natura meramente volontaria.

[51] *US – Tuna II (Mexico)*, *op. cit.*, par. 202.

[52] *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, Organo d'Appello, 24 aprile 2012, WT/DS406/AB/R, (US – Clove Cigarettes), par. 169; *United States – Certain Country of Origin Labelling (COOL) Requirements*, Organo d'Appello, 23 luglio 2012, WT/DS384/AB/R WT/DS386/AB/R, (US – COOL), par. 271.

[53] *US – Clove Cigarettes*, *op. cit.*, parr. 174, 94-95.

[54] *Ivi*, parr. 182, 215; *US – COOL*, *op. cit.*, par. 271. È opportuno osservare che, nel caso EU – *Palm Oil (Malaysia)*, il Panel ha indicato che la natura e il contenuto della valutazione ai sensi dell'art. 2.1 riguardante il trattamento meno favorevole si applicano *mutatis mutandis* alla valutazione e al bilanciamento condotti ai sensi dello *chapeau* dell'art. XX GATT. *European Union and Certain Member States – Certain Measures Concerning Palm Oil and Oil Palm Crop-Based Biofuels (Malaysia)*, Panel, 26 aprile 2024, WT/DS600/R, (EU – Palm Oil (Malaysia), Panel), parr. 7.498, 7.499, 7.1097.

suo sesto considerando, ricalca lo *chapeau* dell'art. XX GATT 1994. Esso, invero, chiarisce che nessun Paese può essere privato della possibilità di adottare misure necessarie alla tutela di un obiettivo legittimo, «ai livelli che ritiene appropriati», purché tali misure non siano applicate in modo da costituire una discriminazione arbitraria o ingiustificabile tra Paesi in cui prevalgono condizioni analoghe, né rappresentino una restrizione dissimulata al commercio internazionale, e siano in ogni caso conformi alle restanti disposizioni dell'Accordo.

Alla luce di tale inquadramento, emerge che l'art. 2.2 integra e specifica la portata dell'art. 2.1, suggerendo che non ogni ostacolo al commercio internazionale risulta vietato, bensì soltanto quelli «non necessari», ossia sproporzionati rispetto agli obiettivi perseguiti o applicati in modo discriminatorio.

L'analisi del «trattamento meno favorevole» ai sensi dell'art. 2.1 non può pertanto prescindere da una valutazione congiunta della giustificazione e proporzionalità della misura, secondo un approccio coerente con la funzione di bilanciamento tra esigenze di liberalizzazione degli scambi e tutela di interessi pubblici legittimi che permea l'Accordo TBT. Il rinvio interpretativo al contenuto del preambolo e all'art. 2.2 del TBT consente al "*even-handedness analysis*", ossia al bilanciamento di interessi che nel sistema del GATT 1994 è rinvenibile nello *chapeau* dell'art. XX, di trovare "applicazione indiretta" anche nel TBT [55]. Invero, l'Accordo TBT, a differenza del GATT 1994, non contempla una clausola generale di eccezione che consenta di giustificare una misura incompatibile con l'obbligo di non discriminazione, sulla base della tutela di obiettivi regolatori legittimi.

Ne deriva che la verifica dell'esistenza di un «trattamento meno favorevole» si articola in due momenti distinti [56]. In primo luogo, occorre accertare se la misura comporti un impatto negativo sui prodotti importati rispetto a quelli nazionali, incidendo sulle condizioni di concorrenza e sull'accesso al mercato; in secondo luogo, è necessario stabilire se tale impatto negativo non sia riconducibile a una «distinzione regolatoria legittima», vale a dire a una misura proporzionata e funzionale al perseguimento di un obiettivo legittimo [57].

Come già anticipato, i PED provenienti da Paesi terzi che non rispettino una o più delle caratteristiche richieste non possono essere immessi nel mercato del-

[55] Per maggiori informazioni riguardo all'interazione tra art. XX GATT e 2.1 TBT cfr. L. TAMIOTTI-D. RAMOS, *Article 2 TBT: Preparation, Adoption and Application of Technical Regulations by Central Government Bodies*, in P-T. STOLL (ed.), *Commentaries on World Trade Law Online*, Brill | Nijhoff, 2022. Si noti tuttavia che pur riconoscendo analogie tra l'art. XX GATT e 2.1 TBT, l'OdA ha messo in guardia contro una trasposizione diretta di tale analisi, sottolineando che si tratta di due disposizioni distinte, ciascuna con una specifica operatività giuridica, cfr. *inter alia*, *EC – Seal Products*, *op. cit.*, par. 5.313.

[56] *US – Clove Cigarettes*, *op. cit.*, par. 169.

[57] *Ivi*, parr. 182, 215; *US – COOL*, *op. cit.*, par. 271.

l'Unione, anche qualora risultino conformi a regimi di cybersicurezza nazionali sofisticati e idonei a prevenire o mitigare gli effetti di attacchi informatici. In tale prospettiva, il CRA, imponendo l'osservanza dei requisiti essenziali di cui all'Allegato I, rischia di determinare l'esclusione di prodotti extra-Ue, sebbene conformi a standard di sicurezza differenti ma potenzialmente equivalenti, con possibili effetti negativi sulla concorrenza dei prodotti importati rispetto a quelli interni. Ne deriva la necessità di esaminare il Regolamento alla luce del principio di non discriminazione, interpretato secondo la nozione di trattamento nazionale.

In considerazione dei passaggi sopra delineati e dei criteri elaborati dal DSB [58], i PED europei ed extra-Ue possono essere considerati agevolmente «prodotti simili», e dunque l'attenzione deve concentrarsi sull'analisi dell'eventuale esistenza di un trattamento meno favorevole a loro carico.

Occorre verificare *in primis* se la misura in esame influisca *de jure* o *de facto* [59] sulle pari opportunità competitive tra i prodotti importati e i prodotti interni simili [60]. Tale valutazione deve essere condotta attraverso l'analisi del design, della struttura e del funzionamento previsto della misura in questione [61].

Sebbene il CRA trovi applicazione in modo uniforme a tutti i PED, indipendentemente dalla loro provenienza, l'obbligo di conformarsi ai requisiti essenziali determinati dall'Unione europea, senza la possibilità di dimostrare l'equivalenza – in termini di efficacia – dei requisiti di cybersicurezza previsti dall'ordinamento del Paese d'origine, può determinare oneri aggiuntivi per gli operatori economici extra-Ue che intendano accedere al mercato europeo.

Tali operatori sono infatti tenuti a sostenere costi supplementari sia di natura

---

[58] Secondo l'interpretazione degli organi di risoluzione delle controversie dell'OMC, la "similitarità" dei prodotti deve essere valutata, tra l'altro, sulla base di quattro criteri generali, e cioè: (i) le proprietà, la natura e la qualità dei prodotti; (ii) gli usi finali dei prodotti; (iii) i gusti e le abitudini dei consumatori – più compiutamente indicati come percezioni e comportamenti dei consumatori – rispetto ai prodotti; e (iv) la classificazione tariffaria dei prodotti, cfr. *inter alia*, *United States – Certain Measures Affecting Imports of Poultry from China*, Panel, 25 ottobre 2010, WT/DS392/R, parr. 7.424-7.427, 7.429; *Indonesia – Certain Measures Affecting the Automobile Industry*, Panel, 23 luglio 1998, WT/DS54/R; WT/DS55/R; WT/DS59/R; WT/DS64/R, par. 14.109; *Philippines – Taxes on Distilled Spirits*, Organo d'Appello, 20 gennaio 2012, WT/DS396/AB/R; WT/DS403/AB/R, parr. 7.31-7.37, 7.124-7.127. DS396/AB/R; WT/DS403/AB/R, parr. 7.31-7.37, 7.124-7.127.

[59] *US – COOL*, *op. cit.*, par. 286.

[60] *United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products (Article 21.5 Mexico)*, Organo d'Appello, 11 gennaio 2019, WT/DS381/AB/RW, (*US – Tuna II (Mexico) (Article 21.5 Mexico)*), par. 7.29.

[61] *United States – Certain Country of Origin Labelling (COOL) Requirements (Article 21.5 – Canada and Mexico)*, Organo d'Appello, 29 maggio 2015, WT/DS384/AB/RW; WT/DS386/AB/RW, (US – COOL (Article 21.5 – Canada and Mexico)), par. 5.15.

amministrativa sia di ulteriore certificazione, al fine di ottenere l'immissione dei prodotti di provenienza extra-Ue sul mercato dell'Unione. In questo contesto, il requisito in esame ben può determinare una distinzione regolatoria tra prodotti nazionali e prodotti importati simili, con possibili implicazioni in termini di impatto negativo sulle condizioni di concorrenza ai sensi dell'art. 2.1 del TBT.

Tuttavia, la mera esistenza di una distinzione regolatoria non implica l'esistenza di un «trattamento meno favorevole» né, dunque, una violazione dell'art. 2.1 TBT. È necessario infatti verificare se l'impatto negativo sui prodotti importati possa essere ricondotto a una «distinzione regolatoria legittima» [62]. Tale passaggio si configura quale momento di bilanciamento volto ad accertare, in conformità alla logica sottesa allo *chapeau* dell'art. XX GATT 1994, se la differenza di trattamento derivante dal regolamento tecnico possa ritenersi proporzionata e giustificata in relazione all'obiettivo legittimo perseguito, ovvero se essa si traduca in una forma di discriminazione arbitraria o ingiustificabile, non spiegabile alla luce di tale finalità.

L'analisi richiede quindi una valutazione accurata del progetto, della struttura, dell'architettura, del funzionamento e dell'applicazione del regolamento tecnico in esame, al fine di stabilire se la misura sia effettivamente equa o se, al contrario, discrimini i prodotti importati [63]. A tal proposito, risulta essenziale concentrarsi sulla natura della distinzione regolatoria. *In primis*, va individuato l'«obiettivo legittimo» sottostante alla misura, a cui segue l'esame del design e delle condizioni della sua applicazione.

Nel caso di specie, l'obiettivo perseguito dal Regolamento riguarda principalmente la protezione della cybersicurezza [64], finalità che può essere agevolmente assimilata alla tutela della sicurezza nazionale [65]. La legittimità di tale obiettivo è rafforzata dal fatto che la sicurezza nazionale [66] viene esplicitamente menzionata come finalità *legittima* nella lista contenuta all'art. 2.2 e nel settimo paragrafo del preambolo del TBT.

Per quanto riguarda la "proporzionalità" della misura, l'OdA ha sottolineato la necessità di valutare se l'impatto negativo dovuto alle distinzioni regolatorie

---

[62] *US – Clove Cigarettes*, *op. cit*., par. 182, 215; *US – COOL, op. cit*., par. 271.

[63] *EU – Palm Oil (Malaysia), Panel, op. cit*., par. 7.498; *US – COOL, op. cit*., par. 271; *US – Clove Cigarettes, op. cit*., par. 182; *US – Tuna II (Mexico)*, *op. cit*., par. 225.

[64] Sebbene il concetto non sia menzionato esplicitamente nel Regolamento, esso può essere facilmente desunto dal contenuto e dai "considerando" ivi contenuti, v. *ex multis* Par. 1-2 Considerando CRA e COMMISSIONE EUROPEA, *Executive Summary of the Impact Assessment Report*, 2022.

[65] N. MISHRA, *op. cit*.

[66] G. GAGLIANI, *op. cit*.

sia «calibrato» in relazione al rischio che la misura mira a prevenire [67].

Alla luce delle analogie tra l'interpretazione dello *chapeau* dell'art. XX del GATT 1994 e dell'art. 2.1 del TBT, considerato anche il linguaggio del sesto considerando del preambolo del TBT, è possibile [68] ricorrere all'analisi giurisprudenziale sviluppata in relazione all'art. XX per orientare la valutazione dell'equità della misura [69]. Assumono dunque particolare rilievo il nesso tra l'eventuale discriminazione e l'obiettivo della misura [70] e la ragione posta alla base della differenza di trattamento [71]. Invero, una discriminazione può essere considerata arbitraria o ingiustificabile quando le motivazioni addotte a giustificazione della stessa risultano prive di una connessione razionale con l'obiettivo della misura, oppure sono in contrasto con tale obiettivo [72].

Nel caso di specie, le distinzioni regolatorie introdotte dal CRA appaiono concretamente correlate all'obiettivo finale perseguito, ossia la tutela della cybersicurezza e, più in generale, della sicurezza nazionale, obiettivo esplicitamente riconosciuto come legittimo dall'art. 2.2 TBT.

Alla luce di tali considerazioni, la discriminazione *de facto* a svantaggio dei PED importati introdotta dal CRA può quindi ritenersi legittima rispetto agli scopi perseguiti.

Inoltre, pur comportando un maggiore onere per gli operatori economici extra-Ue, la misura non pare potersi ritenere una discriminazione arbitraria o ingiustificabile, poiché gli adempimenti richiesti risultano funzionalmente connessi alla prevenzione dei rischi che il Regolamento intende mitigare.

Analoghe considerazioni possono essere estese alle distinzioni regolatorie derivanti dai diversi oneri di certificazione imposti in funzione delle

---

[67] Per maggiori dettagli, cfr. *US – Tuna II (Mexico)*, *op. cit*., par. 297; *US – COOL, op. cit.*, par. 340.

[68] Si noti tuttavia che sebbene l'esistenza di una discriminazione arbitraria o ingiustificabile costituisca un modo per dimostrare la mancanza di equità, non si tratta dell'unico criterio rilevante a tale fine. In altri termini, l'esame di un regolamento tecnico mediante l'applicazione della "connessione razionale" è considerato accettabile, ma non esaurisce necessariamente l'applicazione giuridica dell'art. 2.1 del TBT, cfr. L. TAMIOTTI-D. RAMOS, *op. cit.*; *US – Tuna II (Mexico) (Article 21.5 Mexico)*, *op. cit.*, parr. 7.90-7.92, 7.94-7.96.

[69] Per un approfondimento dell'analisi ai sensi dello *chapeau* dell'art. XX GATT, cfr. G. ADINOLFI, *Article XX GATT [Chapeau]*, in P-T. STOLL (ed.), *Commentaries on World Trade Law Online*, Brill | Nijhoff, 2022.

[70] Si noti che il nesso tra l'eventuale discriminazione e l'obiettivo della misura costituisce uno dei fattori principali, sebbene non l'unico, per accertare l'esistenza di una discriminazione arbitraria o ingiustificabile, cfr. *EC – Seal Products*, *op. cit.*, par. 5.321.

[71] *Brazil – Measures Affecting Imports of Retreaded Tyres*, Organo d'Appello, 17 dicembre 2007, WT/DS332/AB/R, (Brazil – Retreaded Tyres), parr. 226, 227, 246.

[72] *Brazil – Retreaded Tyres*, *op. cit.*, parr. 226, 227, 246.

diverse categorie di PED (di *default* [73] – né importanti né critici –, importanti e critici), nonché al regime meno gravoso in termini certificativi riconosciuto ai PED beneficiari della presunzione di conformità ai sensi dell'art. 27 CRA [74].

In conclusione, le differenze regolatorie introdotte dal CRA non sembrano configurare un «trattamento meno favorevole» ai sensi dell'Accordo TBT; di conseguenza, il Regolamento appare conforme all'art. 2.1 TBT.

3.3. Analisi ai sensi dell'art. 2.2 del TBT

Un ulteriore profilo meritevole di approfondimento concerne la necessità di verificare che il CRA non si traduca in un ostacolo non necessario al commercio internazionale, in linea con i principi di proporzionalità e ragionevolezza sanciti dall'art. 2.2 del TBT. Esso, infatti, prescrive che i Membri dell'OMC debbano garantire che la preparazione, l'adozione e l'applicazione dei regolamenti tecnici non avvengano «con l'intento o con l'effetto di creare ostacoli non necessari al commercio internazionale». Inoltre, devono assicurare che i propri regolamenti tecnici non siano «più restrittivi per il commercio del necessario per raggiungere un obiettivo legittimo, tenendo conto dei rischi derivanti dal mancato conseguimento di tale obiettivo».

In base all'interpretazione giurisprudenziale dell'OdA è richiesto di valutare se il regolamento tecnico sia più restrittivo per il commercio del necessario per conseguire un obiettivo legittimo, tenendo conto dei rischi derivanti dal mancato conseguimento di tale obiettivo. Questo passaggio richiede un esame articolato. Da un lato, occorre identificare l'obiettivo legittimo che il Membro dell'OMC intende perseguire e verificare la sua effettiva legittimità. Dall'altro, è necessario valutare la misura tecnica in relazione alla sua proporzionalità. In particolare, occorre accertare se le restrizioni imposte siano strettamente correlate al raggiungimento dell'obiettivo e se non eccedano quanto necessario per realizzarlo [75].

Tale approccio permette di distinguere tra regolamenti "giustificati", che

---

[73] PARLAMENTO EUROPEO, *EU Cyber-Resilience Act*, 2024.

[74] La presunzione di conformità opera da "ponte" tra la norma astratta (il requisito) e la realtà tecnica del prodotto (la sua progettazione e produzione). In pratica, l'adozione degli standard dell'Unione europea semplifica enormemente la dimostrazione della conformità, poiché non servirebbe sviluppare da zero prove tecniche, né giustificare altre soluzioni.

[75] *Australia – Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging*, Organo d'Appello, 29 giugno 2020, WT/DS435/AB/R; WT/DS441/AB/R, (Australia – Tobacco Plain Packaging (Honduras)), par. 6.3.

perseguono obiettivi legittimi in modo proporzionato, e misure che, pur formalmente legittime, generano effetti sproporzionati sugli scambi internazionali.

Come già emerso nell'analisi precedente, l'art. 2.2 TBT contiene un elenco non esaustivo di obiettivi legittimi, tra i quali ivi rientra, la tutela della sicurezza nazionale. Nel caso di specie, poiché la cybersicurezza può essere agevolmente ricondotta a tale categoria, il requisito può ritenersi soddisfatto.

Per quanto concerne il secondo step dell'esame, l'OdA ha chiarito che la valutazione della necessità di una misura richiede un'analisi relazionale, nota come "test di necessità", che comporta il bilanciamento di tre elementi strettamente interconnessi: (i) il grado in cui la regolamentazione tecnica limita gli scambi commerciali; (ii) il contributo effettivo della misura al conseguimento di un obiettivo legittimo; e (iii) i potenziali rischi derivanti dal mancato raggiungimento dell'obiettivo [76]. Qualora la misura sia preliminarmente considerata "necessaria", è possibile procedere a un'analisi comparativa [77], valutando se esistano soluzioni alternative meno restrittive o più efficaci nel perseguire lo stesso obiettivo, al fine di accertare la proporzionalità e la razionalità della regolazione adottata [78].

Nella definizione del c.d. "test della necessità", l'OdA ha precisato che il termine «necessario» non si limita a ciò che è «indispensabile». Tuttavia, una misura qualificata come necessaria si colloca significativamente più vicina al polo dell'indispensabile, piuttosto che all'estremo opposto rappresentato dal mero contributo al raggiungimento dell'obiettivo legittimo [79].

Per quanto concerne la determinazione del grado di restrittività commerciale, per "restrizione" è da intendersi qualsiasi misura che produca un effetto limitativo sugli scambi internazionali. In secondo luogo, secondo la giurisprudenza dell'OMC, occorre valutare in che misura – o se del tutto – il regolamento tecnico contribuisca effettivamente al conseguimento dell'obiettivo legittimo individuato. Tale valutazione deve considerare il design, la struttura, il funzionamento e l'applicazione concreta della misura, al fine di accertare l'effettivo impatto del regolamento sull'obiettivo [80].

L'OdA ha puntualizzato che l'adempimento ai sensi dell'art. 2.2 non

---

[76] *US – Tuna II (Mexico)*, *op. cit.*, par. 318; *US – COOL, op. cit.*, par. 374; *Australia – Tobacco Plain Packaging (Honduras)*, *op. cit.*, par. 6.3.

[77] Si noti che l'OdA ha chiarito la facoltatività di tale passaggio sulla base delle caratteristiche del caso di specie, cfr. *Australia – Tobacco Plain Packaging (Honduras)*, *op. cit.*, par. 6.4.

[78] *US – COOL (Article 21.5 – Canada and Mexico)*, *op. cit.*, par. 5.199. Per maggiori approfondimenti sull'analisi cfr. L. TAMIOTTI-D. RAMOS, *op. cit.*

[79] *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, Organo d'Appello, 10 gennaio 2001, WT/DS161/AB/R; WT/DS169/AB/R, par. 161.

[80] *US – COOL*, *op. cit*., par. 373.

richiede il pieno raggiungimento dell'obiettivo, poiché, per definizione, un obiettivo legittimo può essere perseguito o conseguito in misura maggiore o minore. Invero, il sesto considerando del TBT stabilisce che ad un Membro dell'OMC non può essere impedito di adottare misure necessarie per conseguire i propri obiettivi legittimi «ai livelli che ritiene appropriati», mentre il settimo considerando conferma il diritto di adottare misure necessarie per la protezione degli interessi essenziali di sicurezza.

Riguardo ai rischi derivanti dal mancato conseguimento dell'obiettivo legittimo, l'art. 2.2 TBT indica un elenco non esaustivo di elementi pertinenti da considerare. Tra questi rientrano, in particolare, le informazioni scientifiche e tecniche disponibili, le tecnologie di trasformazione applicabili e gli usi finali previsti dei prodotti. Questi elementi consentono di valutare la proporzionalità della misura e la sua adeguatezza rispetto agli obiettivi perseguiti, bilanciando la protezione degli interessi legittimi con l'impatto sugli scambi internazionali [81].

Nel caso del CRA, i maggiori oneri gravanti sui PED extra-Ue, derivanti dall'imposizione dei requisiti essenziali europei, sono suscettibili di limitare gli scambi commerciali. Tuttavia, appare evidente che tali requisiti possano risultare altresì efficaci nel ridurre gli incidenti e gli attacchi informatici [82], garantendo così un incremento della cybersicurezza e, di conseguenza, della sicurezza nazionale [83].

Considerata la rilevanza e la sensibilità del tema della sicurezza nazionale, nonché la crescente minaccia rappresentata dagli attacchi e rischi cibernetici [84], pare dunque ragionevole considerare la misura proporzionata alla luce del bilanciamento previsto dall'art. 2.2 TBT.

Come anticipato, l'analisi relazionale può essere integrata da un'analisi comparativa, confrontando la misura oggetto della valutazione con eventuali misure alternative, ragionevolmente disponibili, meno restrittive per il commercio e in grado di apportare un contributo equivalente al raggiungimento dell'obiettivo legittimo. Poiché il CRA impone il rispetto di specifici requisiti, in parte fondati su standard internazionali [85], esso non sembra essere eccessivamente restrittivo se confrontato con altre misure, quali il divieto assoluto di

---

[81] L. TAMIOTTI-D. RAMOS, *op. cit*.

[82] COMMISSIONE EUROPEA, *op. cit*.

[83] Par. 1-2 Considerando, CRA.

[84] K. HUANG-S. MADNICK-N. CHOUCRI-F. ZHANG, *A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade*, in Global Policy, 2021, vol. 12, n. 5, p. 626.

[85] ENISA-JRC, *Cyber Resilience Act Requirements Standards Mapping – Joint Research Centre & ENISA Joint Analysis*, 2024.

importazione, le limitazioni al volume delle merci o dazi doganali elevati, nell'ottica del perseguimento dell'obiettivo di sicurezza.

In sintesi, alla luce delle interpretazioni giurisprudenziali dell'OdA e dell'analisi condotta, il CRA appare conforme ai requisiti dell'art. 2.2 dell'Accordo TBT.

3.4. Osservanza delle disposizioni degli artt. 2.4 e 2.7 del TBT

Uno degli obiettivi dell'Accordo TBT è la promozione dell'armonizzazione degli standard a livello internazionale. Pertanto, diviene necessario esaminare il CRA anche in tale contesto.

L'armonizzazione può essere definita come l'adozione, da parte di più Paesi, di standard e regolamentazioni comuni in una determinata materia, laddove in precedenza ciascuno di essi disponeva di un proprio insieme di requisiti [86]. Ai sensi dell'art. 2.4, i Membri dell'OMC devono «utilizzare gli standard internazionali come base per i propri regolamenti tecnici», salvo che tali standard risultino inefficaci o inadeguati al perseguimento degli obiettivi legittimi [87]. In tale contesto, assume particolare rilevanza il fatto che l'onere della prova circa l'assenza di fondamento su uno standard internazionale grava sulla parte che contesta la coerenza della misura [88].

Il termine «basato su» deve essere inteso in senso ampio. Esso significa che il regolamento tecnico deve essere «fondato su», «basato su», «costruito su» lo standard internazionale [89]. Tuttavia, ciò non significa che i Membri debbano necessariamente rispettare *in toto* lo standard internazionale pertinente. L'obbligo di utilizzare lo standard internazionale rilevante «come base» non è quindi un requisito rigido che impone di uniformare il regolamento tecnico a tale standard. Questa formulazione concede flessibilità ai Membri e riconosce che diversi approcci possono rispettare l'obbligo sancito dall'art. 2.4 TBT. Inoltre, lo stesso prevede che i Membri non sono obbligati a utilizzare standard internazionali come base per i propri regolamenti tecnici «quando tali standard internazionali o le parti pertinenti risultino inefficaci o inadeguati al perseguimento degli obiettivi legittimi prefissati».

L'OdA ha chiarito che tale disposizione implica la necessità di un esame

---

[86] J.P. TRACHTMAN, *Regulatory Jurisdiction and the WTO*, vol. 10, n. 3, in *Journal of International Economic Law*, 2007, pp. 631-651.

[87] E. SHEARGOLD, *op. cit*.

[88] *EC – Sardines*, *op. cit.*, par. 282.

[89] *European Communities – Measures Concerning Meat and Meat Products (Hormones)*, Organo d'Appello, 13 febbraio 1998, WT/DS26/AB/R; WT/DS48/AB/R, parr. 166, 242, 244.

approfondito e di una determinazione sulla legittimità degli obiettivi perseguiti dalla misura [90]. In tale contesto, gli obiettivi legittimi richiamati dall'art. 2.4 devono essere interpretati nel contesto dell'art. 2.2 del TBT.

La giurisprudenza dell'OMC ha inoltre chiarito il significato dei concetti di «inefficace» e «inadeguato» ai sensi dell'art. 2.4 del TBT. In particolare, un mezzo si considera inefficace quando non consegue l'obiettivo legittimo perseguito, mentre è definito inadeguato se non risulta particolarmente idoneo a garantirne il raggiungimento. In altri termini, la questione dell'efficacia riguarda i risultati concreti derivanti dall'impiego dei mezzi, mentre quella dell'adeguatezza attiene alla natura intrinseca degli strumenti adottati [91].

Nel caso del CRA, il rapporto congiunto di ENISA e Joint Research Centre del 2024, intitolato *Cyber Resilience Act Requirements Standards Mapping*, ha provveduto, da un lato, a creare una mappatura sistematica tra i requisiti essenziali del CRA (Allegato I) e gli standard tecnici esistenti; dall'altro, a condurre un'analisi delle lacune (*gap analysis*) per evidenziare in quali aree è necessario lo sviluppo di ulteriori standard armonizzati [92]. La mappatura ha mostrato che, sebbene esistano standard rilevanti come ETSI EN 303 645 (per la sicurezza dei dispositivi *Internet of Things*), EN ISO/IEC 27002:2022 (per i controlli di sicurezza), EN ISO/IEC 29147:2020 (per la *vulnerability disclosure*) ed EN ISO/IEC 30111: 2020 (per la gestione delle vulnerabilità nei prodotti *software*), nessuno di essi è in grado, preso singolarmente, di garantire il livello di protezione perseguito dal CRA e di coprire in modo esaustivo tutti i requisiti dell'Allegato I [93]. Tale indagine sottolinea quindi la necessità di armonizzare e sviluppare standard specifici che possano costituire in futuro strumenti riconosciuti per la presunzione di conformità, ai sensi del Regolamento. In tale contesto, ENISA ha altresì provveduto a mappare specificamente gli esistenti standard internazionali da utilizzare come base per il sistema EUCC [94]. Nel caso in cui la Commissione europea adotti un atto delegato, i sistemi europei di certificazione della cybersicurezza individuati assumerebbero carattere vincolante per i PED critici.

Gli studi hanno pertanto evidenziato come il CRA si fondi in parte sugli standard esistenti e come, al contempo, manchino standard in grado di garantire il livello di protezione perseguito dall'Unione.

---

[90] *EC – Sardines*, *op. cit.*, par. 286.

[91] *EC – Sardines*, *op. cit.*, par. 285.

[92] ENISA-JRC, *op. cit*.

[93] *Ivi*, pp. 6-42.

[94] ENISA-JRC, *op. cit*.; ENISA, *Cyber Resilience Act implementation via EUCC and its applicable technical elements*, 2025.

Nel contesto considerato, assume altresì rilevanza l'art. 2.7 del TBT, che impone ai Membri dell'OMC di considerare positivamente l'accettazione come equivalenti delle regolamentazioni tecniche adottate da altri Membri, anche qualora differiscano dalle proprie, a condizione che soddisfino adeguatamente gli obiettivi perseguiti dalla normativa nazionale. L'equivalenza rappresenta quindi uno strumento meno restrittivo degli scambi per raggiungere un obiettivo legittimo. Tuttavia, il linguaggio dell'art. 2.7 configura un obbligo di buona condotta e "*best efforts*" e non un vincolo rigido. Esso richiede invero solo di «prendere in considerazione positivamente» e non di «accettare» l'equivalenza, lasciando margine di valutazione soggettiva. Inoltre, la decisione di riconoscere come equivalenti le regolamentazioni tecniche di altri Membri si fonda su criteri soggettivi di soddisfazione [95].

Alla luce di quanto esposto, l'assenza di riconoscimento di requisiti esteri – pur potendo garantire un grado di protezione analogo – al fine di rafforzare la cybersicurezza nazionale e l'eventuale obbligatorietà dell'impiego dello schema EUCC in caso di atti delegati della Commissione, può considerarsi giustificata alla luce della sensibilità ed urgenza della materia (cybersicurezza – sicurezza nazionale) e dell'assenza di standard adeguati condivisi. Ne consegue che la mancata equivalenza con regolamentazioni tecniche adottate da altri Membri dell'OMC non deve essere considerata automaticamente come una violazione dell'art. 2.7 dell'Accordo TBT.

Per concludere, l'eventuale introduzione di ulteriori standard relativi ai requisiti essenziali di cybersicurezza, così come il mancato riconoscimento di standard esteri, non possono ritenersi in contrasto con gli artt. 2.4 e 2.7, in considerazione della particolare sensibilità del tema, dell'elevato livello di protezione che l'Unione europea intende perseguire e dell'assenza di standard internazionali idonei a garantire tale livello.

4. Conclusione

Il presente contributo si è confrontato con un profilo al quale la dottrina ha dedicato scarsa attenzione, guardando al possibile impatto del CRA sugli scambi internazionali per accertare se la disciplina così introdotta si ponga in contrasto con gli impegni assunti dall'Unione europea in base all'Accordo sugli ostacoli tecnici facente capo all'Organizzazione mondiale del commercio.

La *ratio* che è alla base di questo Accordo è quella di garantire agli Stati un margine di manovra entro il quale possono perseguire interessi generali anche

[95] L. TAMIOTTI-D. RAMOS, *op. cit*.

definendo le caratteristiche dei beni commercializzati sui rispettivi mercati nazionali, ma senza che ciò si traduca in un mutamento delle condizioni di competitività e in ostacoli non necessari agli scambi internazionali.

La disciplina sostanziale e procedurale posta dal CRA si applica ai prodotti con elementi digitali immessi sul mercato dell'Unione anche laddove essi siano originari da Paesi terzi. Ne derivano, pertanto, specifici obblighi in capo agli importatori e ai rappresentati autorizzati dei fabbricanti esteri, i quali sono tenuti a garantire che i PED prodotti in paesi extra-Ue soddisfino i requisiti essenziali di processo e di prodotto di cui all'Allegato I del Regolamento, siano stati sottoposti alle procedure di valutazione di conformità specificamente individuate rinviando alla normativa dell'Unione già in vigore e, infine, rechino la marcatura CE quale segno distintivo.

Dal confronto con l'Accordo TBT deriva che il CRA risponde pienamente agli obblighi di non discriminazione ivi previsti. Pur comportando un onere aggiuntivo per i fabbricanti esteri, tenuti a sostenere costi supplementari sia di natura amministrativa che di ulteriore certificazione per accedere al mercato dell'Unione, il CRA non applica nei loro confronti un «trattamento meno favorevole» rispetto a quello riservato ai produttori localizzati nel territorio dell'Unione. Pienamente legittimo è infatti, alla luce dell'art. 2.1 dell'Accordo TBT, perseguire un obiettivo di primaria importanza quale quello di garantire la cybersicurezza di beni di uso comune o posti alla base del funzionamento di infrastrutture necessarie all'ordinato svolgimento della vita politica, economica e sociale degli Stati.

Parimenti, non può affermarsi che il CRA si traduca in un ostacolo "non necessario" al commercio internazionale. Nonostante gli effetti restrittivi sulle importazioni, il rispetto dei requisiti essenziali prescritti, nonché l'eventualità che per i PED critici si imponga la conformità a un sistema europeo di certificazione adottato in base al CSA, appaiono strettamente funzionali a garantire la sicurezza dell'Unione europea, la sicurezza nazionale degli Stati membri e risultano proporzionati alla realizzazione di questo obiettivo.

Infine, da un'analisi della prassi che ha preceduto ed accompagnato l'entrata in vigore del CRA risulta evidente come i legislatori europei abbiano tenuto nella dovuta considerazione gli standard internazionali esistenti, integrando la loro disciplina in virtù dell'elevato livello di cybersicurezza perseguito.

Proprio queste circostanze contribuiscono a spiegare come allo stato attuale la legittimità del CRA non sia stata oggetto di particolari contestazioni in seno agli organi politici dell'OMC e non risulti verosimile l'apertura di una controversia innanzi agli organi contenziosi. In definitiva, il CRA dimostra come le regolamentazioni tecniche ben possano costituire degli utili strumenti di politica pubblica finalizzati al perseguimento di interessi generali e non sempre nascondano finalità protezionistiche.

Capitolo 9

Profili informatico-giuridici della cybersicurezza nel procurement sanitario

Marco Mancarella [*]

Abstract: I dispositivi medici in Rete, in uso presso le strutture sanitarie, costituiscono oggi un *enter-point* di particolare interesse per gli attacchi informatici, a fronte del quale non vi sono ancora in Italia adeguate e standardizzate soluzioni di acquisto in sicurezza, tenuto conto anche degli obblighi di *e-procurement* cui devono sottostare gli enti di settore. Il contributo, partendo da una ricostruzione normativa della materia, analizza poi nel dettaglio i profili informatico-giuridici di maggiore interesse nei processi di approvvigionamento dei macchinari medici in Rete, delineando anche una sintetica *roadmap* finale per gli enti, al fine di un adeguato e responsabile approccio alla cybersicurezza dei propri sistemi.

Keywords: Cybersicurezza – Sanità – Procurement – Amministrazione digitale – Codice appalti

1. Introduzione

L'esigenza di garantire elevati standard di sicurezza nel settore sanitario nasce dal profondo impatto che le moderne tecnologie digitali stanno esercitando

[*] Professore Associato di Informatica giuridica (GIUR-17/A), presso l'Università del Salento – Dipartimento SUS, marco.mancarella@unisalento.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

su questo ambito. L'impiego crescente di connettività in Rete, sensori, dispositivi indossabili e sistemi di monitoraggio remoto (*home caring*) ha contribuito alla nascita e alla diffusione della cosiddetta "salute digitale" o "eHealth" [1]. In questo nuovo contesto tecnologico, aspetti come la cifratura dei dati e la protezione dei sistemi da potenziali attacchi informatici sono diventati elementi imprescindibili dell'infrastruttura sanitaria.

I dati statistici degli ultimi anni evidenziano un costante aumento degli attacchi informatici, una tendenza che, almeno finora, non mostra segni di rallentamento. Secondo il Rapporto CLUSIT 2025 [2], nel 2024 la crescita anno su anno degli incidenti rilevati da fonti pubbliche e accertati è stata del 27,4% (da 2.779 a 3.541). Oltre ad osservare una crescita costante della frequenza degli incidenti, la situazione si è evoluta in senso peggiorativo anche dal punto di vista delle loro conseguenze, con un costante incremento della "*severity* media" (indice di gravità) degli incidenti rilevati. Infatti, come nell'anno precedente, anche nel 2024 gli incidenti classificati come "critici" o "gravi" hanno rappresentato circa l'80% del totale (erano il 50% nel 2020), anche se nel 2024 la percentuale di attacchi "*critical*" è diminuita, mentre è aumentata quella degli attacchi con "*severity high*", in particolare per la diminuzione (in media) degli impatti derivanti da attacchi con finalità cybercriminali. Il Rapporto CLUSIT ritiene che i dati siano estremamente chiari nel configurare, rispetto al periodo 2011-2019, un cambiamento drastico nello scenario globale della 'cyber-insicurezza', al quale, visti gli esiti, non è evidentemente corrisposto un incremento sufficiente della consapevolezza, delle risorse allocate e delle contromisure adottate dai difensori.

Particolarmente colpito è stato il settore sanitario, sempre secondo il Rapporto in esame. Infatti, a livello globale, il settore ha registrato 810 cyber incidenti divenuti di pubblico dominio nel 2024, il 30% in più rispetto all'anno precedente e il quadruplo rispetto al 2020 e 2021, con un trend in forte crescita che non accenna a diminuire. Sostanzialmente il 100% degli incidenti (806 incidenti complessivi) ha avuto una motivazione di stampo cybercriminale, mentre solo

---

[1] Per un più ampio approfondimento della materia, si veda: M. MANCARELLA, *eHealth e diritti. L'apporto dell'informatica giuridica*, Roma, Carocci, 2013; C. FARALLI-R. BRIGHI-M. MARTONI (eds), *Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealt*, Torino, Giappichelli, 2015; G. FIORIGLIO, *eHealth: tecnologie, diritto e salute*, in T. CASADEI-S. PIETROPAOLI (eds), *Diritto e tecnologie informatiche*, Milano, Wolters Kluwer, 2021, pp. 45-56; G. MAGLIO, *eHealth*, in M. MANCARELLA, *Lineamenti di Informatica Giuridica*, Trento, Tangram Edizioni Scientifiche, 2024, pp. 293-350.

[2] L'Associazione Italiana per la Sicurezza Informatica, con sede presso il Dipartimento di Informatica "Giovanni Degli Antoni" dell'Università degli Studi di Milano, pubblica annualmente un rapporto di settore. Quello 2025 è disponibile alla pagina web: https://clusit.it/rapporto-clusit/.

una manciata (4 in totale) deriva da attività di *hacktivism* [3] e di *cyber espionage* [4]. L'Europa è il secondo continente, dopo quello americano, ad essere colpito nel settore sanitario.

Il presente lavoro, dunque, si propone di analizzare gli standard di sicurezza applicabili ai dispositivi medici [5] connessi in Rete, con un focus sul modo in cui il rischio cibernetico viene integrato nel processo complessivo di gestione del rischio da parte dei produttori di macchinari e degli altri stakeholder del settore. In particolare, l'analisi si concentrerà sui profili informatico-giuridici di maggiore interesse nei processi di acquisto e valutazione dei sistemi informativi clinico-assistenziali presso le strutture sanitarie, con l'obiettivo di individuare buone pratiche e aree di miglioramento in materia di sicurezza informatica.

2. L'evoluzione del contesto normativo di riferimento: le iniziative europee e i recepimenti nazionali

Nell'ambito dell'attuale quadro normativo, la materia cyber ha assistito

[3] Il termine, utilizzato in Italia anche nella sua forma "hacktivismo", deriva dall'unione delle parole *hacking* e *activism* e indica una tipologia di attivismo effettuato mediante pratiche derivanti dall'azione diretta digitale in stile hacker, solitamente ricorrendo all'uso della pirateria informatica (cfr. P. HIMANEN, *L'etica hacker e lo spirito dell'età dell'informazione*, Milano, Feltrinelli, 2001; S. LEVY, *Hackers. Gli eroi della rivoluzione informatica*, Milano, ShaKe, 1994; G. ZICCARDI, *Etica e informatica. Comportamenti, tecnologie e diritto*, Milano, Pearson Paravia Bruno Mondadori, 2009).

[4] Il termine, utilizzato in Italia anche nella sua forma "spionaggio informatico", indica l'attività di ottenere informazioni segrete o sensibili attraverso l'uso di sistemi informatici, reti e dispositivi digitali senza l'autorizzazione del titolare dei dati.

[5] Per "dispositivo medico", in base al Regolamento (UE) 2017/745, occorre intendere: "Qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie, diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità, studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico, fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi".

All'interno della macrocategoria dei dispositivi medici, merita particolare attenzione la sottocategoria degli apparecchi elettromedicali (ad es. elettrocardiografi (ECG), dispositivi diagnostici come scanner e apparecchiature per raggi X), estremamente esposti ad attacchi informatici. Si intende per "apparecchio elettromedicale", in base alla Norma CEI EN 60601-1, un dispositivo elettrico che trasferisce energia verso o dal paziente, oppure rileva tale trasferimento, con finalità diagnostiche, terapeutiche o di compensazione di una malattia o menomazione.

ad una crescente evoluzione, configurandosi quale vero e proprio fattore di rilevante importanza, sia in ambito europeo che nazionale. L'Unione Europea ha quindi definito e sviluppato una strategia complessa e integrata in risposta all'evoluzione delle minacce digitali e alla crescente interdipendenza delle tecnologie digitali nella vita quotidiana e nelle operazioni economiche. Gli obiettivi principali dei regolamenti, delle direttive e dei provvedimenti sono:

– rafforzare la cybersicurezza: l'UE ha lavorato per migliorare la protezione delle sue infrastrutture digitali da attacchi informatici, promuovendo la cooperazione tra Stati membri e migliorando la resilienza delle reti e dei sistemi informativi;
– proteggere i dati e la privacy: l'UE, a seguito dell'adozione del Regolamento Generale sulla Protezione dei Dati, ha continuato a promuovere politiche per garantire la protezione dei dati personali, sia online che offline;
– regolare l'Intelligenza Artificiale: l'UE ha cercato di stabilire un *framework* regolatorio per l'IA, al fine di stimolare l'innovazione, garantendo al contempo la sicurezza, la protezione dei diritti fondamentali e la trasparenza dei sistemi intelligenti;
– promuovere la resilienza digitale: l'UE a fronte di eventi di alta criticità ha stabilito strategie e misure per garantire che le organizzazioni siano preparate a fronteggiare crisi digitali, che vanno da interruzioni informatiche a disastri legati alle tecnologie.

Pertanto, alla luce della complessità e ormai ampiezza della legislazione, al fine di una maggiore chiarezza di inquadramento della materia, utile per poi approfondire gli obiettivi del presente contributo, di seguito si ripercorre l'evoluzione del quadro normativo in materia di cybersicurezza nell'ordinamento europeo e italiano, offrendo una sintetica panoramica [6].

a) *Framework* europeo:

– Direttiva (UE) 2014/53 (*Radio Equipment Directive* – RED), istituisce un quadro normativo per le apparecchiature radio, stabilendo i requisiti essenziali per la sicurezza e la salute, la compatibilità elettromagnetica (EMC) e l'efficienza dello spettro radio. La direttiva include ora l'art. 3, par. 3, allo scopo di definire i requisiti dei dispositivi in relazione alla *cybersecurity* [7];

[6] Un quadro aggiornato è offerto da: S. PIETROPAOLI, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, Giappichelli, 2025.

[7] Per un approfondimento, si consiglia la lettura di: P.G. CHIARA, *Commission Delegated*

- Regolamento (UE) 2016/679 (*General Data Protection Regulation* – GDPR), il quale impone ai titolari del trattamento di dati personali l'adozione di un sistema di gestione dei dati personali, di cui i produttori e distributori di dispositivi medici, titolari del trattamento, dovranno tener conto, sia all'interno del proprio contesto aziendale, sia con riferimento ai prodotti offerti sul mercato;
- Regolamento (UE) 2017/745 (*Medical Device Regulation* – MDR), il quale ha introdotto cambiamenti significativi nella regolamentazione relativa alla produzione e commercializzazione dei dispositivi medici, elevando gli standard di sicurezza e prestazione. Ha inoltre ridefinito, in modo sostanziale, i compiti e le responsabilità degli operatori economici lungo l'intera filiera, chiamati ora ad assumere un ruolo più attivo e responsabile durante tutto il ciclo di vita del dispositivo. In quest'ottica, l'MDR ha modificato profondamente la normativa precedente, intervenendo su numerosi aspetti: dall'immissione sul mercato alla vigilanza sugli organismi notificati, dalle procedure di valutazione della conformità alle indagini e valutazioni cliniche, fino alla gestione del rischio e alla sorveglianza post-commercializzazione;
- Regolamento (UE) 2017/746 (*In Vitro Diagnostic medical device Regulation* – IVDR), regolamento gemello del Regolamento UE 2017/745 sui dispositivi medici (MDR), rappresenta uno dei cambiamenti più significativi degli ultimi anni nel settore della diagnostica in vitro: esso è stato concepito, per stabilire un quadro normativo solido, trasparente e sostenibile per gli IVD, che si allinei con i progressi tecnologici in ambito medico-diagnostico, senza perdere di vista la salute dei pazienti;
- MDCG 2019-16 (*Guidance on Cybersecurity for Medical Devices*), con la quale il *Medical Device Coordination Group* (MDCG) [8] fornisce indicazioni ai fabbricanti di dispositivi medici per soddisfare i requisiti di *cybersecurity* previsti dal Regolamento (UE) 2017/745 (MDR) e dal Regolamento (UE) 2017/746 (IVDR). In particolare, si concentra su come i fabbricanti possono

Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices (2022) in *European Data Protection Law Review,* vol. 8, n. 1, pp. 103-107.

[8] Il Gruppo di Coordinamento per i Dispositivi Medici (MDCG) si occupa di questioni chiave del settore dei dispositivi medici, dalla supervisione degli Organismi Notificati o dalla standardizzazione alla sorveglianza del mercato, passando per questioni internazionali, nuove tecnologie e indagini cliniche. La sua competenza deriva dalla suddivisione in 13 sottogruppi, che forniscono rispettivamente consulenza e redigono linee guida nel loro ambito di competenza. I membri dei sottogruppi sono nominati dagli Stati membri per un mandato di 3 anni. Le parti interessate e le associazioni con sede in Europa partecipano alle riunioni a seguito di candidature presentate tramite appositi inviti a manifestare interesse. Per ogni approfondimento: https://health.ec.europa.eu/medical-devices-dialogue-between-interested-parties/medical-device-coordination-group-working-groups_en.

garantire la sicurezza dei loro dispositivi medici dal punto di vista informatico, seguendo le disposizioni dell'Allegato I dei regolamenti;
- Regolamento (UE) 2019/881 (*EU Cybersecurity Act*), punta a raggiungere un elevato livello di cybersicurezza, cyber resilienza e fiducia nell'Unione Europea definendo obiettivi, attività e questioni organizzative per una rinominata e rafforzata Agenzia dell'Unione europea per la cibersicurezza (ENISA), con un nuovo mandato permanente; delineando un quadro per i sistemi europei di certificazione volontaria della cybersicurezza dei prodotti, dei servizi e dei processi delle tecnologie dell'informazione e della comunicazione (TIC) e dei servizi di sicurezza gestiti;
- MDCG 2021-25, con il quale il *Medical Device Coordination Group* (MDCG) introduce importanti aggiornamenti per i fabbricanti in merito all'applicazione dei requisiti del Regolamento (UE) 2017/745 (MDR) ai dispositivi *legacy* (immessi sul mercato prima del 26 maggio 2021, conformemente all'art. 120 del MDR) e ai dispositivi *old* (immessi sul mercato prima del 26 maggio 2021, ma non soggetti al MDR);
- Linee guida IMDRF (*Principal and practices for Medical Devices Cybersecurity e Principles and Practices for the Cybersecurity of Legacy Medical Devices*), documento che stabilisce i principi essenziali armonizzati da rispettare nella progettazione e produzione dei Dispositivi Medici (DM) e Medico – Diagnostici in vitro (IVD), allo scopo di garantire sicurezza ed efficacia dei prodotti secondo la propria destinazione d'uso;
- Norme tecniche ISO 14971, ISO 13485, ISO 27001, IEC 80001-1, IEC 62304, IEC 82304-1, tutte pertinenti al settore medicale, in particolare per quanto riguarda la gestione dei rischi, la qualità dei dispositivi medici e la cybersicurezza;
- Direttiva (UE) 2022/2555 (Direttiva NIS2), che coinvolge i fabbricanti di dispositivi medici, specialmente quelli di classe III, IIb e i dispositivi medico-diagnostici in vitro, in quanto considerati elementi critici. La direttiva impone ai fabbricanti di adottare misure per garantire la sicurezza dei loro sistemi e reti informatiche, inclusi quelli relativi alla produzione, sviluppo e manutenzione dei macchinari medicali. Ciò significa che i produttori devono valutare i rischi, implementare misure di sicurezza, gestire gli incidenti e garantire la continuità operativa, anche nella gestione della catena di approvvigionamento;
- Regolamento (UE) 2023/607, estende il periodo di transizione per alcuni dispositivi medici (dispositivi *legacy*[9]) per evitare carenze sul mercato e

[9] I "dispositivi *legacy*" sono i dispositivi medici, dispositivi medici impiantabili attivi e dispositivi medici diagnostici in vitro – coperti da un certificato di direttiva valido – che continueranno ad essere immessi sul mercato dopo la data di applicazione del MDR o del IVDR.

consentire una graduale transizione al nuovo regime del MDR. Il regolamento proroga la validità dei certificati e delle dichiarazioni di conformità delle direttive precedenti, stabilendo nuove scadenze (fino al 31 dicembre 2027 o 2028) e introducendo la cancellazione del periodo di "*sell-off*" per i dispositivi immessi sul mercato prima della scadenza del periodo transitorio;

– Regolamento (UE) 2024/2847 (*Cyber Resilience Act* – CRA), stabilisce requisiti di *cybersecurity* obbligatori per i prodotti digitali (hardware e software) lungo tutto il loro ciclo di vita. L'obiettivo è garantire che questi prodotti siano progettati, sviluppati e mantenuti in modo sicuro, riducendo le vulnerabilità e migliorando la fiducia degli utenti;
– Regolamento (UE) 2024/1689 (*AI Act*), è stato pubblicato sulla Gazzetta ufficiale europea il 12 luglio 2024, aprendo una nuova era per i software basati su sistemi di AI. L'Unione Europea si è posta infatti come obiettivo quello di stabilire, per la prima volta a livello mondiale, le regole per la progettazione, realizzazione e immissione sul mercato dei sistemi di AI. Tali regole poi, troveranno applicazione, non solo nei confronti dei fornitori stabiliti nella Ue, ma anche nei confronti di quelli extra Ue (art. 2, lett. a). In questo modo l'*AI Act* influenzerà la produzione di sistemi AI a livello mondiale;
– Regolamento (UE) 2025/327 (*European Health Data Space* – EHDS), il cui obiettivo è istituire "lo spazio europeo dei dati sanitari prevedendo disposizioni, norme e infrastrutture comuni e un quadro di governance al fine di facilitare l'accesso ai dati sanitari elettronici per l'uso primario dei dati sanitari elettronici e l'uso secondario di tali dati" (art. 1, par. 1).

b) *Framework* italiano:

– D.l. n. 105/2019 (convertito nella l. 18 novembre 2019, n. 133), il quale prevede l'istituzione del c.d. "perimetro di sicurezza nazionale cibernetica", tramite l'inclusione al suo interno delle pubbliche amministrazioni, degli enti e degli operatori nazionali – anche privati – nei casi in cui: a) esercitino una funzione essenziale per lo Stato, oppure forniscano un servizio indispensabile al mantenimento di attività civili ed economiche fondamentali; b) l'esercizio di tale funzione o l'erogazione di tale servizio dipenda da reti, sistemi informativi o servizi informatici, il cui malfunzionamento, interruzione o utilizzo improprio potrebbe compromettere la sicurezza nazionale;
– D.lgs. n. 36/2023 (Codice dei Contratti Pubblici), introduce rilevanti novità in materia di cybersicurezza, con particolare riferimento al settore sanitario. In particolare, l'art. 19 del decreto prevede che le stazioni appaltanti, gli enti concedenti e gli operatori economici partecipanti siano tenuti ad adottare misure tecniche e organizzative adeguate, volte a garantire la cybersicurezza e la protezione dei dati personali nell'ambito delle procedure di gara;

– L. n. 90/2024, la quale mira a rafforzare la cybersicurezza nazionale e a contrastare i reati informatici, recando disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario 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;
– PNRR Missione 6.C2 – 1.1.2. (Ammodernamento del parco tecnologico e digitale ospedaliero – Grandi apparecchiature Sanitarie), che permette di realizzare, mediante Acquisto di nuove Grandi Apparecchiature, il rinnovamento e l'ammodernamento del parco tecnologico delle attrezzature sanitarie obsolete e fuori uso migliorando l'erogazione dei Servizi Sanitari;
– D.lgs. n. 138/2024, recepisce la direttiva NIS2, con l'obiettivo di rafforzare la resilienza delle infrastrutture critiche e dei servizi essenziali contro le minacce informatiche, proteggendo così il funzionamento del mercato interno e la sicurezza nazionale;
– D.p.c.m. 30 aprile 2025, adottato in attuazione dell'art. 14, comma 1, della l. n. 90/2024, definisce – attraverso tre Allegati – le misure operative da adottare nelle attività di approvvigionamento di beni e servizi informatici impiegati in contesti connessi alla tutela degli interessi nazionali strategici. Il d.p.c.m. si inserisce nell'ambito della strategia nazionale di rinforzo della cybersicurezza delle tecnologie utilizzate dalla pubblica amministrazione e reca una disciplina specifica per alcuni appalti pubblici di beni e servizi informatici, ritenuti "cruciali" per il corretto funzionamento dello Stato e delle sue articolazioni e dunque meritevoli di una maggior tutela sul versante cibernetico e informatico. Esso si applica solamente agli appalti pubblici di beni e servizi informatici impiegati in due settori specifici, ovverosia: i) in contesti connessi alla tutela di interessi nazionali strategici; ii) in contesti connessi alla tutela della sicurezza nazionale.

3. Dispositivi medici in Rete: problematiche di interoperabilità e sicurezza

L'impiego di dispositivi medici connessi in Rete è cresciuto in modo esponenziale negli ultimi anni. Queste apparecchiature vengono interconnesse tramite reti di comunicazione – quali LAN o Internet – al fine di abilitare la raccolta e lo scambio di dati e informazioni tra loro, operatori sanitari e pazienti.

Questa evoluzione, sempre più presente nei contesti sanitari, consente di migliorare la qualità e l'efficacia delle cure offerte e di ottimizzare i costi legati

alla gestione dei dati. Tuttavia, la connessione in rete dei dispositivi medici presenta criticità significative: tra queste, la sicurezza e la tutela della privacy dei dati; di talché la standardizzazione e l'interoperabilità dei *device* e delle infrastrutture digitali sono sfide fondamentali.

In particolare, considerando che in Italia la frequenza e la sofisticazione degli attacchi informatici sono in forte aumento, risulta evidente che la protezione e la gestione sicura della connettività dei macchinari sanitari siano aspetti imprescindibili e da non sottovalutare. Eventuali attacchi informatici a una singola struttura sanitaria o all'intero sistema sanitario regionale possono avere conseguenze di diversa gravità. Oltre agli impatti economici – come la necessità di investire risorse per il ripristino dei sistemi compromessi – le conseguenze più rilevanti riguardano la salute dei cittadini. Un attacco potrebbe, infatti, causare interruzioni nei servizi di assistenza, ad esempio bloccando procedure diagnostiche o trattamenti, con potenziali ripercussioni dirette sul benessere dei pazienti. Una prima vittima per un attacco *ransomware*, purtroppo, è stata già registrata nel 2020 in Germania [10].

Per garantire la sicurezza e la privacy dei dati nei dispositivi medici è fondamentale adottare misure protettive sia da parte dei produttori sia degli utilizzatori. I produttori devono integrare la sicurezza fin dalle prime fasi di sviluppo del macchinario (*security by design*) e prevedere impostazioni di sicurezza attive di default (*security by default*), così da offrire una protezione elevata già al momento della messa in servizio. Gli utilizzatori, invece, sono chiamati a gestire con attenzione, ad esempio, l'autenticazione degli utenti, il controllo degli accessi e la modifica periodica delle password.

Un ulteriore aspetto cruciale riguarda la definizione e l'adozione di standard e protocolli di comunicazione condivisi tra apparecchi o dispositivi. Nel contesto sanitario, la capacità di diversi macchinari di scambiarsi informazioni in modo corretto e sicuro – ad esempio dati clinici o istruzioni terapeutiche – è essenziale. L'impiego di protocolli differenti può causare errori di trasmissione o di interpretazione, con potenziali conseguenze gravi sulla salute dei pazienti. Al contrario, l'uso di protocolli comuni facilita l'integrazione degli apparecchi o dispositivi all'interno di sistemi più complessi, come reti di monitoraggio o sistemi informativi sanitari, aumentando l'efficienza complessiva e riducendo il rischio di errori dovuti a problemi di compatibilità.

---

[10] L'Ospedale universitario di Duesseldorf. il 10 settembre 2020, ha subito un attacco informatico, causato da una vulnerabilità dei *gateway* Citrix, denominata CVE-2019-19871. Il motivo del decesso è dovuto al fatto che l'ospedale non ha potuto accettare i pazienti a causa dell'attacco e la donna è stata mandata in una struttura sanitaria più distante. Il trasferimento è stato fatale per la paziente. Per un approfondimento della notizia: https://www.cybersecurity360.it/nuove-minacce/ransomware/donna-morta-per-colpa-di-ransomware-la-sanita-non-cyber-sicura-uccide/.

4. Gli standard di sicurezza imposti dal Regolamento (UE) 2017/745

La crescente consapevolezza delle sfide tecnologiche, in particolare del rischio di attacchi informatici rivolti a dispositivi medici sempre più complessi e connessi, ha spinto il Legislatore europeo a rafforzare le difese contro gli attacchi malevoli, estendendo le garanzie di sicurezza a tutto il ciclo di vita del dispositivo, non limitandole alla sola fase di progettazione.

Sebbene il Regolamento (UE) 2017/745 non utilizzi esplicitamente il termine "cybersecurity", esso contiene numerose disposizioni volte a proteggere i dispositivi medici da accessi non autorizzati e a prevenire alterazioni delle loro funzionalità che possano compromettere la salute e la sicurezza di pazienti e utilizzatori, oltre a salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni gestite.

In particolare, tra i requisiti generali di sicurezza e prestazione elencati nell'Allegato I del Regolamento (UE) 2017/745, si stabilisce che i dispositivi medici debbano essere sicuri ed efficaci nelle normali condizioni d'uso, senza compromettere né lo stato clinico dei pazienti né la sicurezza e la salute degli utilizzatori e di altre persone eventualmente coinvolte. Ciò implica che progettazione e produzione devono rifarsi allo stato dell'arte scientifico e tecnologico, garantendo che i rischi residui associati all'impiego del dispositivo siano accettabili in rapporto ai benefici attesi per i pazienti e compatibili con un elevato livello di protezione della salute e della sicurezza. Pertanto, i fabbricanti sono tenuti a implementare fin dalla progettazione un sistema di gestione del rischio volto a limitare al minimo i rischi e a prevenire incidenti, includendo sia le problematiche di sicurezza (*security issues*), quali la protezione da intrusioni esterne, sia quelle relative alla sicurezza clinica (*safety issues*), attraverso valutazioni di rischio e misure di controllo appropriate.

Oltre alle misure di sicurezza *by design* e relative all'ambiente IT, è indispensabile adottare strategie efficaci di sorveglianza e vigilanza sulla cybersicurezza dei dispositivi anche dopo la loro commercializzazione. Data la rapidità con cui evolvono le minacce e le vulnerabilità nel settore biomedico, le difese iniziali possono rapidamente risultare obsolete o insufficienti rispetto al livello di rischio-beneficio accettabile. Per questo motivo, il fabbricante è responsabile di implementare e mantenere aggiornato un sistema di sorveglianza post-commercializzazione che monitori anche gli aspetti di cybersecurity. Come previsto dall'art. 83 del Regolamento (UE) 2017/745, tale sistema si basa sulla raccolta e analisi delle informazioni sulla qualità, prestazioni e sicurezza del dispositivo, raccogliendo dati provenienti da diversi attori, quali utenti, distributori, importatori e rappresentanti autorizzati, al fine di aggiornare il sistema di gestione del rischio e attuare tempestivamente eventuali azioni preventive o correttive per

eliminare difformità o altre situazioni indesiderabili in relazione alla natura e ai rischi del dispositivo.

Nel corso dei successivi paragrafi si procederà all'analisi delle procedure di acquisto dei dispositivi medici connessi in Rete, quindi vulnerabili, approfondendo, in particolar modo, i profili informatico-giuridici di maggiore interesse nel sistema di acquisto degli stessi e la relativa disciplina, con lo scopo di definire una griglia minima di compliance in tema di *cybersecurity* per le fasi di *procurement*, all'interno delle strutture sanitarie nazionali.

5. La cybersicurezza nel prisma dei contratti pubblici

Negli ultimi anni, il sistema normativo italiano ha assistito a un crescente intreccio tra la disciplina dei contratti pubblici e la cybersicurezza. Attraverso una serie di interventi legislativi succedutisi in tempi ravvicinati, il Legislatore ha inteso rafforzare in modo significativo la tutela della cybersicurezza anche nell'ambito delle procedure di affidamento e di esecuzione dei contratti pubblici [11].

Il nuovo art. 19 del Codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36) ha assunto un ruolo centrale nel delineare i principi guida in materia di digitalizzazione e sicurezza nei procedimenti di gara. Dottrina autorevole [12] ha definito questa disposizione come un vero e proprio "manifesto di politica di cybersicurezza", in quanto enuncia chiaramente gli orientamenti che devono ispirare l'azione delle stazioni appaltanti in ambito digitale.

Al comma 1, l'art. afferma che le amministrazioni aggiudicatrici devono garantire l'esercizio dei diritti di cittadinanza digitale [13], operando secondo i

---

[11] Per un approfondimento più ampio della tematica, rispetto ai contenuti del presente scritto incentrato sui profili informatico-giuridici: T. COCCHI, *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*, n. 1, 2024; G. SFERRAZZO, *La cybersicurezza nel nuovo Codice dei contratti pubblici: l'art. 108, co 4 e le criticità per le stazioni appaltanti*, in *Teoria e Critica della Regolazione Sociale*, n. 1, 2025, pp. 157-179.

[12] S. ROSSA, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, in *Rivista interdisciplinare sul Diritto delle Amministrazioni Pubbliche*, fasc. 2/2024, p. 342, disponibile all'URL: https://ceridap.eu/pdf/estratti/Estratto-10.13130_2723-9195_2024-2-29.pdf.

[13] Per un approfondimento sul tema, si consiglia la lettura della Guida sui diritti di cittadinanza digitali pubblicata nel 2018 dall'Agenzia per l'Italia Digitale – AgID, in attuazione dell'art. 17, comma 1-*quinquies*, del Codice dell'Amministrazione Digitale (d.lgs. n. 82/20055): https://www.agid.gov.it/sites/agid/files/2024-07/Guida_dei_diritti_di_cittadinanza_digitale.pdf.

principi di neutralità tecnologica, trasparenza, protezione dei dati personali e sicurezza informatica. Tale enunciazione assume una portata programmatica e costituisce un riferimento interpretativo fondamentale per le successive scelte applicative. Più operativa è la previsione di cui al comma 5, ove si stabilisce che le stazioni appaltanti e gli enti concedenti devono: adottare misure tecniche e organizzative volte a garantire la cybersicurezza dei sistemi e dei dati; curare la formazione nonché l'aggiornamento continuo del personale addetto alla gestione delle procedure digitali e alla protezione delle informazioni trattate. In tal modo, il Codice dei contratti pubblici introduce una responsabilità strutturale e organizzativa in capo alle amministrazioni, volta non solo al rispetto delle norme tecniche, ma anche alla creazione di una cultura della cybersicurezza.

Passando ora all'analisi del contenuto dell'art. 108, comma 4, del Codice dei contratti pubblici, esso rafforza ulteriormente la centralità della cybersicurezza, imponendo alle stazioni appaltanti di tenere conto di elementi di cybersicurezza nella valutazione dell'elemento qualitativo dell'offerta, ai fini del miglior rapporto qualità-prezzo. Tale valutazione assume carattere prioritario nei contesti in cui l'appalto riguarda interessi strategici nazionali, ponendo così, la cybersicurezza, tra i fattori determinanti nella scelta del contraente.

Ovviamente, nessun discorso in termini di approvvigionamento di apparecchi medicali ha un senso se non collocato nella cornice delle piattaforme di e-procurement e della loro certificazione AgID.

A tal proposito, la disciplina di riferimento è contenuta nell'art. 26 del Codice dei contratti pubblici, che disciplina i requisiti e la certificazione delle piattaforme digitali per l'approvvigionamento.

Il testo vigente (dopo il correttivo con d.lgs. n. 209/2024, recante "Disposizioni integrative e correttive al codice dei contratti pubblici, di cui al d.lgs. 31 marzo 2023, n. 36") affida all'AgID, d'intesa con l'Autorità Nazionale per l'Anticorruzione e la Trasparenza – ANAC, la Presidenza del Consiglio (Dipartimento per la trasformazione digitale) e l'Agenzia per la Cybersicurezza Nazionale – ACN, il compito di stabilire i requisiti tecnici delle piattaforme, definire le modalità di certificazione, nonché quello di curare l'integrazione con la Banca dati nazionale dei contratti pubblici.

Un ulteriore sviluppo normativo si rinviene nel citato d.lgs. n. 138/2024, che recepisce la Direttiva (UE) 2022/2555 (NIS 2).

L'art. 24, comma 2, impone ai cosiddetti soggetti NIS (essenziali e importanti) l'obbligo di adottare misure volte a garantire la sicurezza della catena di approvvigionamento, incluse le relazioni con fornitori e subfornitori. Tale previsione assume rilevanza diretta anche per le procedure ad evidenza pubblica, in quanto comporta una valutazione a monte del rischio cyber derivante dall'intero ecosistema di fornitura, incidendo sulle modalità di selezione dei fornitori e sulle clausole contrattuali.

Altra norma di particolare interesse nell'analisi che stiamo conducendo è contenuta nell'art. 14 del d.lgs. 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".

L'art. in questione, infatti, contiene la norma di snodo che congiunge in modo sistematico la cybersicurezza con la disciplina dei contratti pubblici. La disposizione, dalla formulazione articolata e complessa, introduce obblighi specifici e stringenti in capo alle stazioni appaltanti e agli operatori economici.

L'art. 14 si pone, dunque, come norma cardine in un'ottica di prevenzione e gestione del rischio cyber, richiedendo alle amministrazioni un salto di qualità organizzativo, oltre ad una maggiore consapevolezza nella valutazione degli impatti che le vulnerabilità digitali possono avere sull'esecuzione degli appalti e sui servizi erogati ai cittadini.

In via preliminare, non può non rilevarsi una certa perplessità sul piano sistematico. L'art. 14 introduce, infatti, una disciplina di settore che, pur riguardando gli appalti pubblici, trova collocazione al di fuori del Codice dei contratti pubblici, che costituisce la fonte organica e unitaria per la regolazione della materia. L'introduzione di una normativa autonoma, seppur con finalità speciali, rischia di generare interferenze interpretative e difficoltà di coordinamento, sia sotto il profilo soggettivo (identificazione delle amministrazioni competenti), sia sotto quello oggettivo (ambito di applicazione della norma).

L'art. 14 è espressamente finalizzato all'introduzione di una disciplina speciale per i contratti pubblici relativi a beni e servizi informatici impiegati in contesti connessi alla tutela degli interessi nazionali strategici. Secondo quanto riportato nella relazione tecnica al disegno di legge, la norma mira a rafforzare le tutele di cybersicurezza nelle procedure di approvvigionamento ICT, nei casi in cui queste siano funzionalmente legate alla salvaguardia degli interessi strategici del Paese. Questo obiettivo si innesta coerentemente con quanto già previsto dal Codice dei contratti pubblici, il quale – come noto – impone alle stazioni appaltanti di considerare gli elementi di cybersicurezza nell'ambito della valutazione qualitativa dell'offerta (art. 108, comma 4). Tuttavia, l'art. 14 amplia e rafforza tale previsione, delineando un quadro normativo più rigoroso per i contratti "strategici".

Uno degli aspetti più problematici della disposizione è rappresentato dall'utilizzo, senza una definizione normativa compiuta, della categoria degli "interessi nazionali strategici". Tale nozione costituisce criterio di applicabilità della norma, nel senso che, *a contrariis*, l'art. 14 non si applica agli appalti ICT privi di connessione con tali interessi. Tuttavia, il concetto stesso di "interesse nazionale strategico" resta giuridicamente incerto e frammentato, pur essendo richiamato in più occasioni nell'ordinamento. Tra i riferimenti utili:

– gli artt. 5 e 7 del d.l. n. 82/2021, istitutivo dell'Agenzia per la cybersicurezza

nazionale (ACN), che attribuiscono all'Agenzia la funzione di garante della cybersicurezza connessa a «prodotti e processi informatici di rilevanza strategica»;
– il d.l. n. 21/2012 (convertito con modificazioni dalla l. n. 56/2012), relativo ai poteri speciali nei settori della difesa, energia, trasporti e comunicazioni;
– il d.l. n. 187/2022 (convertito con modificazioni dalla l. n. 10/2023), che interviene sulle attività produttive di rilevanza strategica.

Nonostante l'abbondanza di riferimenti settoriali, manca tuttora una nozione ordinamentale unitaria e sistematica. Questo deficit definitorio genera incertezza e apre margini di discrezionalità applicativa, con potenziali ricadute in termini di contenzioso e inefficienza operativa.

La formula utilizzata dalla l. n. 90/2024 ("interessi nazionali strategici") sembra più ampia rispetto ad altre categorie contigue, come quella di "sicurezza nazionale" utilizzata nel d.l. n. 105/2019 sul Perimetro di sicurezza cibernetica nazionale [14]. Il rischio è, dunque, quello di una inflazione semantica che complica ulteriormente la tassonomia normativa in materia.

La seconda nozione chiave richiamata dall'art. 14 è quella di "elementi essenziali di cybersicurezza", già presente anche nell'art. 108, comma 4, del Codice dei contratti pubblici. A differenza della categoria precedente, questa riceve, nel corpo dell'art., una definizione normativa espressa, che contribuisce – almeno in parte – a ridurre le ambiguità interpretative.

Ai sensi dell'art. 14, per "elementi essenziali di cybersicurezza" si intende: "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 degli interessi strategici". Tale definizione ha il pregio di ancorare la valutazione a parametri tecnici oggettivi, in linea con i principi fondamentali della *security by design* e con le disposizioni europee (in particolare la NIS 2).

L'art. 14 della l. n. 90/2024 rappresenta, senza dubbio, un passo importante verso il consolidamento del legame tra cybersicurezza e contrattualistica pubblica. Tuttavia, la sua effettiva efficacia dipenderà dalla capacità del sistema di chiarire e circoscrivere le nozioni chiave da cui dipende la sua applicazione.

---

[14] Di tale parere: S. Rossa, *Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*, cit., p. 354. L'Autore evidenzia che tale interpretazione estensiva degli interessi nazionali strategici "pare essere confermata dall'art. 10, comma 1 e comma 3 del citato d.d.l. 16 febbraio 2024. Nell'elencare coloro i quali sono tenuti a rispettare gli elementi essenziali di cybersicurezza nelle procedure di aggiudicazione dei beni informatici, la norma menziona due distinte tipologie di soggetti: quelli indicati all'art. 2, comma 2, d.lgs. n. 82/2005 […] e quelli privati previsti dall'art. 1, comma 2-*bis*, d.l. n. 105/2019 ma non ricompresi nel menzionato art. 2, comma 2, d.lgs. n. 82/2005 […]".

Rimane fondamentale distinguere tra gli "elementi essenziali di cybersicurezza", richiamati dall'art. 14 della l. n. 90/2024, e i più generici "elementi di cybersicurezza" menzionati nell'art. 108, comma 4, del Codice dei contratti pubblici.

Il concetto di essenzialità, infatti, presente solo nell'art. 14, risulta poco chiaro e di difficile definizione, generando incertezza interpretativa.

L'art. 14 individua come destinatari le pubbliche amministrazioni, i gestori di servizi pubblici e le società controllate (come definite dal d.lgs. n. 175/2016), facendo esplicito riferimento all'art. 2, comma 2, del Codice dell'Amministrazione Digitale – CAD (d.lgs. n. 82/2005) che elenca tali categorie di soggetti. Quindi, l'elenco risulta molto ampio e – come evidenziato durante i lavori preparatori – rischia di estendere l'applicazione della norma anche a soggetti che non operano in ambiti direttamente legati alla cybersicurezza o alla tutela di interessi strategici nazionali (come alcune scuole o enti locali minori).

Il terzo comma dell'art. 14 estende ulteriormente l'ambito applicativo, includendo anche i soggetti privati che rientrano nel "Perimetro di sicurezza nazionale cibernetica" (art. 1, d.l. n. 105/2019). Si tratta di soggetti privati, con sede in Italia, che svolgono funzioni essenziali per lo Stato o erogano servizi fondamentali per la collettività, e il cui malfunzionamento potrebbe compromettere la sicurezza nazionale.

L'art. 14, al comma 2 [15] rafforza il peso degli aspetti di cybersicurezza all'interno delle gare pubbliche imponendo alle stazioni appaltanti di tenere sempre conto degli elementi essenziali di cybersicurezza nella valutazione della componente qualitativa dell'offerta, conferendo al tema della cybersicurezza un ruolo prioritario, anche nel caso di aggiudicazione al minor prezzo ed, altresì, concedendo alle stazioni appaltanti di escludere offerte che non rispettino i requisiti fissati nel decreto attuativo previsto dal comma 1, avvalendosi delle facoltà previste dagli artt. 107 e 108 del Codice dei contratti pubblici.

Le disposizioni dell'art. 14 della l. n. 90/2024 appaiono in parte ridondanti rispetto a quanto già previsto dall'art. 108 del Codice dei contratti pubblici.

In particolare, il comma 2 dell'art. 14, al punto b), come detto, dispone l'obbligo per le stazioni appaltanti – comprese le centrali di committenza – di tenere conto degli elementi di cybersicurezza nella valutazione dell'elemento qualitativo, qualora il contesto riguardi la tutela degli interessi nazionali strategici: tale obbligo, però, è già espressamente previsto dal comma 4 dell'art. 108.

Anche la previsione contenuta alla lett. d) del comma 2 dell'art. 14 – che

[15] L'art. 14, al comma 2, della l. n. 90/2024, prevede che "nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza: a) possono esercitare la facoltà di cui agli artt. 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al d.lgs. 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1 […]".

impone un tetto massimo del 10% per il punteggio economico nel caso di offerta economicamente più vantaggiosa – ricalca quanto già disposto dallo stesso art. 108, comma 4, rendendo l'intervento normativo, in questo punto, sostanzialmente duplicativo.

Diversamente, alla lett. c) del secondo comma dell'art. 14, il legislatore introduce una novità sostanziale: l'obbligo di inserire gli elementi di cybersicurezza tra i requisiti minimi dell'offerta anche nel caso di aggiudicazione secondo il criterio del minor prezzo, ampliando così l'ambito applicativo delle tutele previste dall'art. 108, comma 4. Questa estensione, tuttavia, avrebbe trovato una collocazione più coerente direttamente all'interno del Codice dei contratti pubblici, anziché in una norma esterna.

6. Il processo di acquisto delle apparecchiature medicali

La tendenza a concentrare gli acquisti delle amministrazioni pubbliche in un numero ristretto di soggetti, operanti come centrali di committenza – ovvero centri specializzati nell'acquisto di beni e servizi destinati ad altri enti, o stazioni appaltanti che stipulano contratti per conto di terzi – è oramai consolidata da tempo. Ed invero, nel settore sanitario, la nascita di enti aggregatori non rappresenta una novità assoluta. Già a partire dalla metà degli anni 2000, alcune legislazioni regionali avevano introdotto il concetto di centrale di committenza, di fatto anticipando la formalizzazione dell'istituto all'interno del Codice dei contratti pubblici del 2006.

L'ambito dei soggetti appaltanti è definito dall'art. 1, comma 2, del d.lgs. n. 165/2001: nel settore sanitario rientrano, tra le amministrazioni aggiudicatrici, il Ministero della Salute, le Regioni, le Aziende sanitarie locali (ASL), le Aziende ospedaliere (considerate organismi di diritto pubblico), nonché le Case di cura e riposo (enti pubblici riconosciuti e gestori di risorse statali).

Una peculiarità che distingue le Aziende sanitarie dalla maggior parte delle altre amministrazioni pubbliche è la loro natura aziendale: si configurano infatti come imprese pubbliche con una vocazione manageriale orientata all'esterno. Questo si riflette nell'adozione della contabilità economico-patrimoniale, in contrasto con quella finanziaria di tipo autorizzatorio tipica di altri enti, spesso privi di una missione aziendale vera e propria. Le Aziende sanitarie, dunque, operano nel contesto del libero mercato della produzione di servizi sanitari, perseguendo criteri di efficienza economica e obiettivi di risultato.

Tuttavia, in passato, l'ampia autonomia gestionale di cui godevano ha rappresentato un punto critico del sistema. In particolare, l'utilizzo incontrollato di

procedure dirette per l'acquisizione di beni e servizi ha contribuito all'aumento incontrollato della spesa pubblica. Ciò è stato favorito dalla frammentazione della domanda e dalla carenza di un controllo sistemico sugli investimenti e sulle loro componenti.

Per contrastare queste storiche disfunzioni, le più recenti tendenze del sistema sanitario puntano su due direttrici principali:

a) l'aggregazione della domanda e dell'offerta;
b) l'efficientamento delle strutture pubbliche responsabili degli acquisti.

Tale prassi risponde all'esigenza, ampiamente condivisa, di rendere più efficiente ed efficace il processo di approvvigionamento pubblico. Ciò avviene, da un lato, attraverso l'aggregazione della domanda, che consente un aumento del potere negoziale della pubblica amministrazione e, di conseguenza, condizioni economiche più vantaggiose sul mercato; dall'altro, mediante una maggiore professionalizzazione del personale operante nelle stazioni appaltanti centralizzate, accompagnata da una razionalizzazione e semplificazione delle procedure di acquisto.

Tali elementi contribuiscono complessivamente a ridurre i costi legati all'organizzazione delle gare, con benefici particolarmente significativi per gli enti di piccole dimensioni.

L'analisi dei canali di acquisto, condotta da AGID [16], evidenzia una chiara tendenza verso una progressiva riduzione del peso delle Centrali di committenza regionali e, ancor più marcatamente, delle gare dirette. Al contrario, si registra una significativa crescita nell'utilizzo degli strumenti messi a disposizione da Consip [17]. In tal senso, Consip stipula accordi quadro con società fornitrici che si impegnano a garantire le loro prestazioni a favore delle stazioni appaltanti che decidono di ricorrervi. Gli enti del Servizio Sanitario Nazionale hanno, infatti, l'obbligo di ricorrere alle convenzioni delle centrali di acquisto territoriali di riferimento o, in mancanza, della Consip. Tuttavia, nel caso in cui non vi siano delle convenzioni concluse da Consip o dalla centrale acquisti territoriali di riferimento, gli stessi devono comunque ricorrere agli strumenti di acquisto e negoziazione telematici messi a disposizione da Consip (MePA, Sdapa, Gare in ASP) o dalla centrale di riferimento.

---

[16] AGID, *La spesa ICT nella PA italiana – Percorsi e trend in atto 2022-2025*, in https://www.agid.gov.it/sites/agid/files/2025-05/Rapporto_La_spesa_ICT_nella_PA_2024.pdf.

[17] Consip è la centrale di acquisto nazionale – interamente partecipata dal Ministero dell'Economia e delle Finanze (MEF) – che offre, attraverso gare e mercati digitali, soluzioni di *e-procurement* per gli acquisti delle amministrazioni pubbliche. Consip è stata istituita con il d.m. 24 febbraio 2000, in esecuzione dell'art. 26 della l. 23 dicembre 1999, n. 488.

Nel dettaglio, la quota della spesa ICT delle ASL veicolata tramite contratti Consip è aumentata dal 42% del 2021 al 49% del 2024. Parallelamente, il ricorso a gare dirette si è ridotto, passando a rappresentare il 32% della spesa, con un calo di cinque punti percentuali nel biennio 2023-2024. Anche il ruolo delle Centrali di committenza regionali risulta in flessione, con una quota prevista pari al 24% della spesa complessiva. Per quanto riguarda le Aziende Ospedaliere, la quota di spesa ICT gestita tramite Consip era inizialmente inferiore rispetto alle ASL (38% nel 2021), ma è in forte crescita, fino a superare il 50% nel periodo 2023-2024. Le gare dirette, che rappresentavano il 38% nel 2021, sono scese al 35% nel 2022 e al 27% nel biennio successivo. Anche per queste strutture si osserva una riduzione dell'incidenza delle Centrali di committenza regionali, con una quota che passa dal 24% al 21%.

Complessivamente, l'analisi conferma una crescente centralizzazione degli investimenti, trainata in particolare dalle aggiudicazioni delle gare legate alla Sanità Digitale.

7. Conclusioni: come assicurare la cybersicurezza negli acquisti

Seppur Consip, negli ultimi anni, nell'ambito delle procedure di acquisto delle c.d. apparecchiature medicali (ed in particolare, da ultimo, relativamente all'"Investimento M6C2 1.1 Ammodernamento del parco tecnologico e digitale ospedaliero del sub-investimento M6C2 1.1.2 – Grandi Apparecchiature – Milestone M6C2-00-ITA1"), abbia pubblicato oltre nove procedure di gara, prevedendo nei capitolati aspetti tecnici e clinici delle apparecchiature condivisi con le Società Scientifiche di riferimento (SIRM, AIFM, AIMN), di fatto spingendo gli Operatori Economici ad offrire apparecchiature di ultima generazione, caratterizzate dai più elevati e innovativi standard tecnologici, anche in termini di cybersicurezza, nonché includendo l'inserimento dei criteri delle schede DNSH (*Do No Significant Harm*) – rispetto ai quali gli Operatori Economici hanno sia autocertificato e comprovato con opportuna documentazione il possesso dei requisiti previsti *ex ante* esecuzione dell'opera, sia rilasciato l'impegno a soddisfare i requisiti *ex post* – si riscontra, allo stato attuale, l'assenza di capitolati specifici riguardanti la definizione di standard minimi di cybersicurezza che i fornitori devono rispettare per partecipare alle gare.

Ed allora, avuto riguardo al quadro attuale, al fine di operare un'azione preventiva e contenitiva del rischio tecnologico connesso alla gestione delle apparecchiature medicali – in attesa dell'effettiva implementazione degli obblighi previsti dalla l. n. 90/2024 a carico delle centrali di committenza – appare

opportuno adottare misure di facile attuazione, finalizzate a garantire un livello più elevato di cybersicurezza nei processi di approvvigionamento e utilizzo di tali apparecchi o dispositivi.

Com'è facile intuire, la fase cruciale – per quanto rileva – è certamente quella dell'acquisizione, nella quale il produttore si interfaccia con l'amministrazione sanitaria al fine di definire e verificare l'implementazione dei requisiti specifici per la fornitura – sia essa di prodotti che di servizi (manutenzione) – la valutazione dei fornitori e l'integrazione degli aspetti tecnici all'interno del *framework* di sicurezza definito dall'amministrazione stessa.

Durante tale fase, a parere di chi scrive e tenuto conto di quanto sinora esposto, l'amministrazione sanitaria deve condurre una duplice valutazione:

1) una valutazione accurata del fornitore/produttore, analizzando la criticità di tale soggetto sulla base dei requisiti di sicurezza definiti nelle proprie *policy* e procedure operative, considerando:
– l'esistenza di un sistema di gestione della sicurezza delle informazioni o almeno la conformità a standard internazionali;
– l'adozione di controlli specifici per la gestione delle attività rivolte alle strutture sanitarie, data la natura sensibile dei dati trattati;
– la chiarezza nella definizione di ruoli e responsabilità in materia di sicurezza delle informazioni;
– il rispetto delle clausole contrattuali legate alla sicurezza;
– le procedure per la segnalazione tempestiva di eventuali vulnerabilità successivamente rilevate;
– la corretta gestione dei sub-fornitori e verifica della loro aderenza agli standard di sicurezza richiesti;
– la conformità alle normative analizzate nel presente scritto, prime tra le quali la NIS2 e il GDPR;
2) una valutazione dei requisiti di sicurezza dei prodotti e servizi, chiedendo al fornitore/produttore la documentazione che attesti la sicurezza *by design* e la gestione del rischio secondo le prassi aziendali e considerando:
– un'azione di *penetration test* e scansioni di vulnerabilità condotti durante sviluppo e produzione;
– la compatibilità e integrazione del dispositivo con il servizio fornito nell'ambiente operativo ospedaliero;
– l'attribuzione dei profili utente in base ai ruoli;
– una modalità di accesso sicuro;
– le prove di conformità alle principali normative e ad eventuali requisiti aggiuntivi stabiliti;
– con riserva dell'amministrazione sanitaria nel condurre autonomamente *audit* o *assessment* per verificare sul campo l'effettiva presenza ed efficacia dei

controlli di sicurezza adottati, salvaguardando così il proprio livello di cybersecurity.

La realizzazione di tali valutazioni, ovviamente, non comporta un'automatica ed assoluta cybersicurezza, ma di certo denota *accountability* e conoscenza degli strumenti giuridico-informatici necessari per assicurare una minore vulnerabilità del sistema sanitario nazionale. Esigenza, oramai, indifferibile.

Capitolo 10

Cybersicurezza e *cyber deception*: sfide e prospettive processualpenalistiche

Mariagisa Landolfi [*]

Abstract: Pensata come strategia di difesa, ad oggi la *cyber deception* costituisce uno strumento prezioso per rafforzare i livelli di *cybersecurity*, poiché funzionale a prevenire e gestire eventuali attacchi informatici. Tuttavia, in ragione delle sue peculiarità operative e, in particolare, della sua capacità di raccogliere dati, essa ben si presta pure a scopi di accertamento e repressione dei reati. In questa prospettiva, si intende vagliare la configurabilità della tecnica in parola nell'ambito del procedimento penale in relazione non solo alle potenzialità informative che ne derivano, ma anche ai rischi per la tenuta delle garanzie processuali.

Keywords: *Cybersecurity* – *Cyber deception* – *Entrapment* – Investigazioni – Processo penale

Sommario: 1. Una breve premessa: la centralità della cybersecurity nel panorama attuale. – 2. Il fascino della *cyber deception*. – 3. I risvolti delle strategie decettive: qualche considerazione di ordine sistematico. – 4. Sui profili di rischio di *entrapment*. – 5. Il modello delle *undercover operations*. – 6. Il ruolo dei soggetti privati: quali prospettive? – 7. Alcune considerazioni (non) conclusive.

[*] Assegnista di ricerca in diritto processuale penale (IUS/16), presso il Dipartimento di Scienze Giuridiche, Università di Bologna, mariagisa.landolfi@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU. Lo studio è frutto di una riflessione sviluppata in sinergia con il gruppo di ricerca che, all'interno del progetto EcoCyber, si occupa dell'analisi di nuove tecniche di *cyber deception*. L'obiettivo è offrire un contributo giuridico che possa risultare utile alle fasi di implementazione degli strumenti decettivi. Si ringrazia l'ing. Silvio Russo, dottorando di ricerca presso il Dipartimento di Informatica – Scienza e Ingegneria, Università di Bologna, per il prezioso confronto sugli aspetti tecnici e operativi.

1. Una breve premessa: la centralità della cybersecurity nel panorama attuale

Negli ultimi anni si è assistito a un progressivo aumento delle minacce informatiche, divenute peraltro ancor più insidiose. Non è un caso, infatti, che il settore del *cybercrime* sia annoverato tra le prime cinque *key areas* dell'ultimo rapporto annuale di *Eurojust*: come si evince chiaramente dai dati, l'Agenzia, nel 2024, si è confrontata con un numero di casi di criminalità informatica maggiore del 25% rispetto a quelli occorsi nell'anno precedente [1].

Un elemento da non sottovalutare è quello fornito dal *report* annuale di *ENISA*: per il 2024, il livello di minaccia alla *cybersecurity* dell'Ue è stato classificato come "sostanziale" [2]. A incidere su tale assestamento sono, tra gli altri, anche le *malicious cyber activities*, divenute sovente una componente all'interno di disegni di *hybrid threat* [3] di più ampia portata. Gli Stati membri, inoltre, continuano ad essere bersaglio di «*cybercriminals, state-aligned threat groups and hacktivists*», che, da parte loro, dimostrano una progressiva evoluzione delle tecniche adoperate [4].

---

[1] In particolare, «*in 2024, cybercrime remained one of the top five crime areas handled by the Agency. Eurojust dealt with 25% more cybercrime cases in 2024 compared to the previous year, almost half of which were newly opened*». Secondo il rapporto *Clusit* sulla *Cybersecurity in Italia e nel mondo* del 2025, «nel 2024 la crescita anno su anno degli incidenti rilevati da fonti pubbliche è stata del 27,4% (da 2.779 a 3.541)», con una situazione evolutasi in senso peggiorativo pure rispetto alle conseguenze. «Come già nel 2023, nel 2024 gli incidenti classificati come "critici" o "gravi" hanno rappresentato circa l'80% del totale (erano il 50% nel 2020), anche se nel 2024 la percentuale di attacchi "*critical*" è diminuita, mentre è aumentata quella degli attacchi con *severity* "*high*", in particolare per la diminuzione (in media) degli impatti derivanti da attacchi con finalità cybercriminali». Inoltre, si osserva che il *cybercrime* fa da sfondo alla maggior parte degli incidenti: «[n]el 2024, infatti, la criminalità cyber è responsabile di quasi 9 attacchi su 10», evidenziando la tendenza delle attività delittuose a puntare «sempre più sul cyberspazio».

[2] ENISA, *2024 Report on the State of the Cybersecurity in the Union*, 3 dicembre 2024.

[3] Pur a mente della complessità definitoria del concetto di *hybrid threats*, esso si riferisce a «*the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare*»; così Commissione europea, Comunicazione congiunta al Parlamento europeo e al Consiglio, *Joint Framework on countering hybrid threats. A European Union response*, JOIN/2016/018 final, 6 aprile 2016. Tra i diversi mezzi adoperabili a tale scopo, possono figurare la manipolazione delle informazioni, gli attacchi informatici, l'influenza o la coercizione economica, manovre politiche occulte, la diplomazia coercitiva oppure minacce di ricorrere alla forza militare. Per un primo inquadramento sul tema, G. GIANNOPOULOS-H. SMITH-M. THEOCHARIDOU, *The Landscape of Hybrid Threats: A conceptual model*, EUR 30585 EN, Publications Office of the European Union, Lussemburgo, 2021.

[4] ENISA, *2024 Report on the State of the Cybersecurity in the Union*, 3 dicembre 2024.

Tali evidenze non fanno altro che riflettere una realtà di fondo: oltre alle più comuni attività relative alla vita personale, lavorativa e sociale delle persone, a essere traslata sul piano digitale è altresì la perpetrazione di condotte criminose, amplificate dalle potenzialità tecniche che la stessa rete mette a disposizione e dall'estensione della superficie di attacco. Eppure, al di là del contesto per così dire "dematerializzato" – che si discosta dai tradizionali canoni spazio-temporali –, gli effetti prodotti sono assolutamente concreti, impattando sugli individui, sulla collettività e, non da ultimo, sulle istituzioni.

La dimensione *cyber*, dunque, ha assunto una posizione centrale e strategica, alla quale si è associata l'esigenza di ripensare le modalità di difesa dalle azioni malevoli. Ne è sintomatico l'importante percorso avviato dall'Unione europea per il rafforzamento del livello di sicurezza delle reti e dei sistemi informativi, da una parte, e di protezione dei dati, dall'altra. Basti pensare, in tal senso, alla *EU Cybersecurity Strategy 2020-2025* e al *Cyber Blueprint* per la gestione delle crisi informatiche, nonché alla crescente produzione normativa, tra cui, primi tra tutti, il *Cybersecurity Act* [5], le due direttive *NIS* e *NIS2* [6] e il più recente *Cyber Resilience Act* [7].

Parallelamente, l'ambiente tecnologico ha imposto un cambio di passo pure rispetto alle misure repressive: oltre a definire fattispecie di reato meglio attagliate al contesto *cyber*, è divenuto prioritario dotarsi di strumenti efficaci nel loro perseguimento.

Anche sotto questo profilo, gli interventi sono stati molteplici, tra i quali pare doveroso rammentare quantomeno la Convenzione di Budapest che, già nel 2001 [8], si proponeva di approntare una risposta alle emergenti minacce

---

[5] Reg. (UE) 2019/881 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, che abroga il reg. (UE) 526/2013.

[6] Rispettivamente: dir. (UE) 2016/1148 del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, recepita con d.lgs. 18 maggio 2018, n. 65; e dir. (UE) 2022/2555 del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del reg. (UE) n. 910/2014 e della dir. (UE) 2018/1972 e che abroga la dir. (UE) 2016/1148, recepita con d.lgs. 4 settembre 2024, n. 138.

[7] Reg. (UE) 2024/2847 del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i reg. (UE) 168/2013 e (UE) 2019/1020 e la dir. (UE) 2020/1828.

[8] Convenzione sulla criminalità informatica (ETS no. 185), 23 novembre 2001, Budapest, ratificata dall'Italia con l. 18 marzo 2008, n. 48. Sulle implicazioni sul piano interno si vedano M.L. Di Bitonto, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. internet*, 2008, 5, p. 503 ss.; L. Lupária, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa: I profili processuali*, in *Dir. pen. proc.*, 2008, p. 696 ss.; L. Lupária (a cura di),

informatiche attraverso la previsione di un quadro di tutela sostanziale e processuale "aggiornato", e, in tempi più recenti, la Convenzione sulla criminalità informatica adottata dalle Nazioni Unite nel 2024 [9]. Sul versante europeo, è indicativa l'attenzione riservata alle prove elettroniche, che ha condotto all'adozione del reg. (UE) 2023/1543 (c.d. *e-evidence*); quest'ultimo, invero, ha introdotto delle procedure volte a facilitarne la raccolta transfrontaliera proprio in ragione dell'estrema volatilità dei dati [10].

Nonostante l'impegno profuso sul piano regolatorio, è inequivocabile che, da solo, esso non sia sufficiente a fronteggiare la costante trasformazione delle minacce cibernetiche, rese sempre più sofisticate dall'impiego di tecniche avanzate di persistenza e dissimulazione e dell'intelligenza artificiale. A questa evoluzione, perciò, corrisponde un necessario sviluppo anche delle strategie di difesa, che non possono più limitarsi a misure passive di prevenzione e resistenza all'attacco, ma che ben possono articolarsi in approcci dinamici e proattivi, capaci di anticipare, neutralizzare e adattarsi in tempo reale ai pericoli emergenti, integrando tecnologie avanzate, analisi predittive e cooperazione interistituzionale.

2. Il fascino della *cyber deception*

In questo contesto si inserisce la *deception*, tecnica di origini risalenti nel tempo, ampiamente sperimentata e utilizzata in rapporto a operazioni di tipo militare e di *intelligence*. In linea di massima, essa consiste nel ricorso all'inganno quale arma di difesa attiva, con l'obiettivo di confondere il nemico e ottenere così un vantaggio tattico [11].

Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest, Giuffrè, Milano, 2009.

[9] Nonostante i buoni propositi che hanno animato la Convenzione sulla criminalità informatica delle Nazioni Unite, il testo, licenziato il 24 dicembre 2024, ha sin da subito mostrato dei profili di criticità, soprattutto in relazione ad alcune previsioni processuali e al loro impatto sulle garanzie fondamentali. Sul tema, L. BARTOLI, *Cybersecurity and the Fight against Cybercrime: Partners or Competitors?*, in *European Journal of Risk Regulation*, 2025, p. 506 ss.

[10] Come è noto, il reg. (UE) 2023/1543 del 12 luglio 2023, attraverso l'introduzione degli ordini di conservazione e produzione delle *electronic evidence* i cui destinatari sono direttamente i *service providers*, intende mettere a disposizione delle autorità giudiziarie nazionali uno strumento che, nel contesto dei procedimenti penali e dell'esecuzione di pene detentive, agevoli e velocizzi l'accesso ai dati, anche se localizzati altrove, per evitarne la cancellazione.

[11] La *deception* è destinata ad avere maggiori possibilità di successo quando vengano adottate misure ampie e coordinate per gestire tutte le fonti convenzionali di *intelligence*, «*including open*

Nella sua declinazione in ambito *cyber*, la *deception* ha portato con sé un importante cambio di paradigma, aprendo la strada a nuove prospettive di protezione della rete e dei sistemi connessi [12]. Di fronte alla "staticità" delle misure di difesa tradizionali, quali ad esempio i *firewall* e gli *antivirus*, si è scorta l'opportunità di impiegare strategie più "dinamiche" in grado di rilevare tempestivamente i pericoli, di studiare e modellare il comportamento dell'avversario, nonché di contenere la sua azione e gli eventuali danni.

L'approccio in parola fa leva su una logica ingannatoria: le infrastrutture di rete vengono strumentalmente arricchite di elementi simulati e/o risorse fittizie per deviare l'attenzione dell'attaccante. Tali componenti sono intenzionalmente costruite in modo da apparire credibili all'esterno, anche rispetto alle possibili vulnerabilità. Da una parte, dunque, si intende schermare gli *asset* effettivamente considerati strategici; dall'altra, invece, si tenta di pilotare la condotta malevola in un ambiente "controllato", in cui la percezione informativa dell'avversario viene compromessa.

Ma vi è di più. Una volta permeato l'ecosistema decettivo, le interazioni dell'aggressore permettono di carpire informazioni sulle sue intenzioni, sugli strumenti che sta adoperando e sulle sue competenze tecniche. Tutti questi elementi fungono da base conoscitiva per fortificare lo scudo difensivo e aumentare la resilienza del sistema.

Molteplici possono essere le tattiche adoperate, anche in combinazione tra loro, che, a seconda dei casi, consentono di intervenire nelle diverse fasi dell'attacco: allo stadio preliminare, ad esempio, si può incidere sull'individuazione delle aree di vulnerabilità; nel corso dell'esecuzione, invece, si può simulare un accesso apparente per indurre l'attaccante a esporsi; ancora, nel momento "esfiltrativo", si possono reindirizzare i dati sottratti verso contenuti esca o tracciabili.

Più nel dettaglio, tra le tecniche più diffuse si annovera, in prima battuta, la

---

sources, such as independent news reporting, signals interception, diplomatic reporting, aerial reconnaissance, and agent observation». Tanto che, là dove le predette cinque componenti siano controllate o comunque monitorate, «*an adversary's ability to verify intelligence is diminished to the point where deception may play a significant part in the success of a particular undertaking*»; così N. WEST, *Historical Dictionary of International Intelligence*, Rowman & Littlefield Publishers, Incorporated, 2015, p. 95.

[12] Sulle opportunità di impiego delle strategie di *cyber deception* in ottica difensiva, Q. ZHU, *The Doctrine of Cyber Effect: An Ethics Framework for Defensive Cyber Deception*, in *ArXiv abs/2302.13362*, 2023, p. 3. Nell'ottica di sviluppare un nuovo approccio basato sulla «*strategic dynamic deception*» e sulle relative potenzialità in termini di difesa delle infrastrutture informatiche, S. RUSSO-C. ZANASI-M. COLAJANNI, *Cyber Defense Through Strategic Dynamic Deception*, in C. KWAN-N. GRATZER-K. PODIŅŠ-M. TOLPPA (a cura di), *2025 17th International Conference on Cyber Conflict: The Next Step (CyCon)*, CCDCOE Publications, Tallinn, 2025, pp. 227-244.

perturbation, che si caratterizza per la capacità di produrre intenzionalmente del "rumore" informativo in modo da distorcere la cognizione dell'aggressore e, dunque, impattare sulle sue scelte. Diversa, invece, è la *moving target defence*, che consiste nella modifica continuativa delle superfici di attacco e delle configurazioni di rete, sistemi e indirizzi IP. Vi sono poi, tra le altre, il *signaling*, vale a dire l'uso strategico di informazioni per influenzare il comportamento dell'attaccante, senza modificare la struttura della rete sottostante, e il *masking*, tecnica che nasconde informazioni sensibili aggiungendo attributi o rumore [13].

Certamente uno dei metodi più noti di *cyber deception* è il *decoying*. Si tratta di "trappole digitali", ossia strutture fittizie pensate per attirare i soggetti malintenzionati e monitorare le azioni da loro perpetuate, incluse le tattiche, le tecniche e gli strumenti impiegati. Un esempio è dato dagli *honeypot* [14], ma anche dagli *honeynet* e *honeytoken*, i quali agiscono simulando, nel primo, un sistema o un servizio ovvero, rispettivamente nella seconda e terza ipotesi, una rete o un elemento esca.

L'*honeypot*, in particolare, si presenta come un possibile bersaglio di attacco, reso intenzionalmente attrattivo per il soggetto esterno, ma al contempo credibile, poiché riproduce vulnerabilità e comportamenti verosimili. L'*hacker*, dunque, invece che aggredire un sistema "reale", finisce per penetrare quello "fittizio", il quale gli restituisce informazioni apparentemente plausibili, ma in concreto prive di valore. Nel mentre, non solo restano intatti gli elementi strategici, ma l'interazione del soggetto esterno con l'*honeypot* permette all'attaccato di rafforzare le proprie difese e di studiare le caratteristiche dell'aggressore.

Alla luce di quanto detto, si comprende come la strategia decettiva permetta di ottenere materiale conoscitivo sia per il destinatario dell'azione intrusiva che per colui che l'ha condotta, ma con un'importante precisazione.

Dal punto di vista del primo, "catturare" un *hacker* tramite un *honeypot*, ad esempio, significa poter monitorare, senza rischiare di compromettere gli *asset* di valore dell'infrastruttura, l'attività perpetuata e procurarsi così preziose

---

[13] Sulle tecniche di *cyber deception*, si rimanda in modo più preciso a C. GONZALEZ-P. AGGARWAL-E.A. CRANFORD-C. LEBIERE, *Adaptive Cyberdefense with Deception: A Human–AI Cognitive Approach*, in T. BAO-M. TAMBE-C. WANG (a cura di), *Cyber Deception. Advances in Information Security*, Springer, Cham, 2023, p. 43 ss.; P.B. LÓPEZ-M.G. PÉREZ-P. NESPOLI, *Cyber Deception: State of the art, Trends, and Open challenges*, in *IEEE Communications Surveys and Tutorials*, 2025; S. SINGH-S. ARORA-S. KAMBOJ, *Harnessing Cyber Entrapment for the Detection of Emerging Internet Threats*, in *Nanotechnology Perceptions*, 2024, v. 20, S15, p. 2827 ss.

[14] In altri termini, si verifica che: «*you create a resource that has no production value or authorized activity. This means if any packet or any interaction is attempted with your honeypot, it's most likely a probe, scan, or attack. This model's very simplicity is its inherent advantage*»; così L. SPITZNER, *The Honeynet Project: Trapping the Hackers*, in *IEEE Security & Privacy*, aprile 2003, p. 18.

informazioni. In primo luogo, possono trarsi indicazioni sul *pattern* comportamentale dell'attaccante e sulle tecniche adottate, che ne disvelano i movimenti, quanto cercato e gli strumenti adoperati, nonché il suo livello di capacità tecnica. Si aggiungono, poi, i dati relativi all'attacco, quali l'orario, la durata, la frequenza, e, non meno importanti, quelli tecnici in senso stretto, vale a dire relativi all'indirizzo IP, alle porte di rete utilizzate, agli strumenti e ai *software* impiegati, ai comandi eseguiti. Ad ogni modo, è utile precisare che la disponibilità di questi elementi può dipendere da diversi fattori, tra cui, *in primis*, la strategia di *cyber deception* utilizzata, la profondità della simulazione e la durata e frequenza dell'attacco.

Dalla diversa prospettiva dell'attaccante, gli scenari variano a seconda dell'obiettivo preposto. Tendenzialmente, però, quando il sistema di *cyber deception* funziona, le informazioni cui l'*hacker* perviene sono solo fittizie.

Degli eventi occorsi, inclusa la difesa decettiva come effettuata, si tiene traccia nel *report* automaticamente generato dal sistema. Esso costituisce un documento di estrema rilevanza per ricostruire i passaggi operativi che si sono susseguiti, soprattutto nei casi in cui la condotta del soggetto esterno non si sia limitata ad accedere ed esportare dati, ma li abbia anche cancellati.

3. I risvolti delle strategie decettive: qualche considerazione di ordine sistematico

Alla luce delle caratteristiche che si è provato brevemente a mettere in risalto, è chiaro come la *cyber deception* costituisca ad oggi una delle più raffinate e promettenti strategie di difesa nel panorama della cybersicurezza. Al contempo, la sua capacità di intercettare informazioni la rende uno strumento potenzialmente performante pure per l'attività di contrasto, nell'ottica sia di prevenire che di reprimere le condotte illecite.

Tuttavia, se ci si sposta nel contesto penale, prima ancora di interrogarsi sull'*an* e sul *quomodo* del suo utilizzo a fini investigativi o anche preventivi, la *cyber deception* pone delle delicate questioni qualificatorie di natura sostanziale e di inquadramento sistematico.

Dall'angolo prospettico dei reati informatici, un primo interrogativo sorge con riferimento all'incidenza sulla configurabilità della fattispecie tipizzata dall'art. 615-*ter* c.p. per l'accesso abusivo a un sistema informatico; più nel dettaglio, il problema attiene alla verifica dell'offensività della condotta perpetuata dall'agente. Si è detto, infatti, che, là dove le misure decettive operino proficuamente, a essere oggetto di incursione non è l'ambiente "reale", quindi il bene

giuridico protetto, ma solo quello "simulato", che nulla contiene se non quanto strumentalmente si intende far trovare.

La questione evoca la categoria del reato impossibile, il quale, come noto, presuppone che l'azione sia posta in essere e, ciononostante, ne difetti l'idoneità offensiva, tanto da rendere impossibile il pregiudizio rispetto all'interesse tutelato dalla fattispecie di reato [15].

A ben vedere, però, nel caso in esame non sembra potersi accedere a una simile lettura. Il ricorso alla *cyber deception*, invero, non dovrebbe essere considerato come la predisposizione di un sistema o di un *software* altro rispetto a quello che si vuole proteggere. Essa, piuttosto, è una misura di sicurezza che si aggiunge all'infrastruttura nel suo complesso, con il chiaro intento di rafforzarne le difese. Sicché, quand'anche l'azione sia stata rivolta contro un reticolo artificiale privo di valore, si è comunque verificata un'intrusione nel perimetro *cyber* non legittima che, come tale, assume rilevanza sotto il profilo penale.

Si potrebbe ritenere, però, che il fatto in esame integri l'autonoma ipotesi di tentativo di cui all'art. 56 c.p., non potendosi trascurare che, ferma l'intenzione dell'agente di penetrare l'infrastruttura, l'intrusione si sia da ultimo realizzata "solo" con riferimento alla porzione "fittizia" che la difende e, dunque, le manovre volte ad aggirare le misure di sicurezza non siano interamente riuscite [16]. In tal caso, è comunque indispensabile che gli atti siano idonei e diretti in modo inequivocabile a commettere l'accesso illegittimo, benché l'azione non giunga a completarsi. In proposito, deve tuttavia darsi atto di un orientamento che riconosce all'accesso abusivo a un sistema informatico la natura di reato di pericolo, con la conseguente difficoltà di ritenere configurabile un'ulteriore anticipazione della soglia di punibilità rispetto alla lesione materiale del bene giuridico protetto [17].

---

[15] Così F. MANTOVANI, *Diritto penale*, Wolters Kluwer-Cedam, Milano, 2020, p. 207. Più diffusamente, sul reato impossibile, il cui referente normativo risiede nell'art. 49 c.p., si veda *ex multis* G. NEPPI MODONA, *Reato impossibile*, in *Dig. disc. pen.*, XI, Torino, 1996; S. RIONDATO, sub *art. 49*, in G. FORTI-S. SEMINARA (a cura di), *Commentario breve al codice penale*, Wolters Kluwer-Cedam, Milano, 2020, p. 393 ss.

[16] Partendo dall'idea, accolta dal legislatore del codice penale, che non possa esservi reato senza offesa ai beni giuridici, l'art. 56 c.p. individua l'autonoma fattispecie del tentativo che sussiste, anche se l'azione non si compia o l'evento non si verifichi, là dove gli atti compiuti dall'agente siano idonei a commettere un delitto, vale a dire «se creano un pericolo per il bene tutelato dalla norma incriminatrice di parte speciale», così G. MARINUCCI-E. DOLCINI, *Manuale di diritto penale. Parte generale*, Giuffrè, Milano, 2015, p. 433. Pur considerata la vastissima letteratura sul tema, si richiamano *ex multis* F. MANTOVANI, *Diritto penale*, p. 468 ss.; E. MORSELLI, *Tentativo*, in *Dig. disc. pen*., XIV, Torino, 1999, p. 198; L. PISTORELLI, sub *art. 56*, in G. FORTI-S. SEMINARA (a cura di), *Commentario breve al codice penale*, cit., p. 455 ss.

[17] Nel senso di ammettere la configurabilità dell'ipotesi tentata, V. DESTITO, *Reati informatici*,

4. Sui profili di rischio di *entrapment*

Provando a osservare il fenomeno della *cyber deception* in relazione al sistema processualpenalistico, a richiedere una più attenta riflessione è proprio la particolare modalità attraverso cui detta strategia viene realizzata: ci si riferisce alla messa a punto di un apparato che è appositamente progettato per risultare interessante agli occhi dell'*hacker*, affinché quest'ultimo colpisca l'organizzazione in un punto preciso. Così descritto, lo schema pare condividere alcuni tratti di fondo con l'istituto dell'*entrapment*, vale a dire con quei metodi investigativi adoperati dalle autorità che presentano profili di rischio di provocazione del reato e che, in quanto tali, trovano un limite *in primis* nel diritto a un equo processo.

Nel provare ad affrontare la questione, può essere utile richiamare l'elaborazione offerta dalla Corte europea dei diritti dell'uomo che, partendo dalla garanzia sancita dall'art. 6 della Convenzione, ha progressivamente tracciato una linea di demarcazione sempre più netta tra le condotte consentite agli agenti "infiltrati" e quelle modalità operative che, ancorché da loro impiegate per finalità di giustizia, danno luogo a condotte istigatorie.

Se, da un lato, è pacificamente ammesso, soprattutto per alcune particolari tipologie di reato, il ricorso a "metodi di indagine speciali", incluse le operazioni *undercover*, dall'altro è altrettanto chiaro come le attività delle autorità non possano spingersi fino a determinare in altri l'azione criminosa. A ostare è non solo la garanzia del *fair trial*, ma più in generale il principio di buona amministrazione della giustizia [18].

Ne discende che dette procedure investigative "extra-ordinarie" debbano essere circoscritte entro precisi limiti [19]. Anzitutto, nell'ottica dell'art. 6 CEDU, a

---

in *Dig. disc. pubbl.*, 2010; N. MAIORANO, sub *art. 615*-ter, in G. LATTANZI-E. LUPO (a cura di), *Codice Penale. Rassegna di giurisprudenza e di dottrina*, vol. V, Giuffrè, Milano, 2022, p. 606. In giurisprudenza, si veda Cass., sez. V, 30 ottobre 2023, n. 43780, che, pur non riscontrando il tentativo, non ne esclude la configurabilità. Per contro, esso non è ritenuto ammissibile da C. PECORELLA, sub *art. 615*-ter, in E. DOLCINI-G.L. GATTA (a cura di), *Codice penale commentato*, IV ed. Wolters Kluwer, Milano, 2015, p. 607.

[18] Corte EDU, 5 febbraio 2008, *Ramanauskas c. Lituania*, par. 53, ove si precisa: «*while the rise in organised crime requires that appropriate measures be taken, the right to a fair trial, from which the requirement of the proper administration of justice is to be inferred, nevertheless applies to all types of criminal offence*». Insomma, «*[t]he right to the fair administration of justice holds so prominent a place in a democratic society that it cannot be sacrificed for the sake of expedience*».

[19] Invero, la giurisprudenza della Corte di Strasburgo, pur ammettendo la possibilità di fare affidamento, in una fase del tutto preliminare e quando il caso lo richiede, su questo genere di fonte, prescrive che «*the subsequent use of such sources by the trial court to found a conviction*

considerarsi permissibili sono solo gli "speciali" mezzi di indagine di matrice essenzialmente passiva – che, quindi, non esercitino un'influenza tale da indurre la perpetrazione di un reato che il soggetto non avrebbe altrimenti commesso o, comunque, di uno più grave di quello che intendeva realizzare in assenza di istigazione –, posti in essere dalle autorità allo scopo di consentire l'accertamento dell'illecito, fornire la prova della sua esistenza e perseguirne l'autore.

Nella prassi, tuttavia, il distinguo non sempre appare immediato, soprattutto in ragione della varietà di situazioni che possono verificarsi. La Corte di Strasburgo ha individuato, ormai da tempo, due parametri tesi a guidare la valutazione: uno di ordine materiale, l'altro di tipo procedurale [20].

Quanto al primo, esso copre molteplici fattori, quali, tra gli altri, i motivi a fondamento dell'operazione e la condotta tenuta dagli agenti. Questi ultimi, in particolare, devono limitarsi ad "aderire" all'attività delittuosa o a "infiltrarsi" nella stessa, ma non anche a iniziarla [21]. Ancora, può venire in considerazione la circostanza che vi siano «sospetti oggettivi» per ritenere che la persona sia coinvolta in attività criminali o predisposta a commettere un reato [22]. Inoltre, il ricorso a simili strumenti di indagine è subordinato alla sussistenza di regole chiare e precise circa l'autorizzazione, l'attuazione e il controllo [23]. Sotto il profilo procedurale, deve altresì essere garantito all'individuo, nel corso del suo

---

is a different matter and is acceptable only if adequate and sufficient safeguards against abuse are in place», quali, in particolare, regole chiare e prevedibili per l'autorizzazione, l'esecuzione e il controllo; così Corte EDU, 5 febbraio 2008, *Ramanauskas c. Lituania*, par. 53.

[20] In proposito deve richiamarsi *in primis* Corte EDU, 9 giugno 1998, *Teixeira de Castro c. Portogallo*, parr. 34-39, cui sono seguite molteplici sentenze che, partendo dallo schema ivi delineato, hanno continuato a precisare i criteri di valutazione in tema di provocazione. Per un approfondimento, A. VALLINI, *Il caso Teixeira De Castro davanti alla Corte Europea per i Diritti dell'Uomo ed il ruolo sistematico delle ipotesi legali di infiltrazione poliziesca*, in *Leg. pen*., 1999, p. 197. Sulle perduranti difficoltà di discernere l'*entrapment*, J.R. SPENCER, *Entrapment and the European Convention on Human Rights*, in *Cambridge Law Journal*, 2001, vol. 60, n. 1, pp. 30-33.

[21] Più nel dettaglio, si rimanda a Corte EDU, 9 giugno 1998, *Teixeira de Castro c. Portogallo*, parr. 34-39, nonché a Corte EDU, 24 giugno 2008, *Milinienė c. Lituania*, parr. 37-38. Ancora, tra i fattori presi in considerazione può rientrare anche la verifica sulle circostanze dell'iniziativa dell'agente di contattare il soggetto; in tal senso, Corte EDU, 15 dicembre 2009, *Burak Hun c. Turchia*, par. 44.

[22] Tali indici trovano espressione in Corte EDU, 4 novembre 2010, *Bannikova c. Russia*, par. 38.

[23] A precisarlo è, ancora una volta, Corte EDU, 9 giugno 1998, *Teixeira de Castro c. Portogallo*, par. 38. Guardando all'ulteriore casistica affrontata dai giudici di Strasburgo, si è affermato che travalica i limiti delle operazioni consentite l'ipotesi in cui non vi siano né autorizzazioni né controlli formali dell'operazione sotto copertura, così Corte EDU, 28 giugno 2018, *Tchokhonelidze c. Georgia*, par. 51.

processo, di poter dedurre utilmente la provocazione, tramite eccezione o in altro modo; profilo, questo, che si aggiunge al rispetto delle garanzie di carattere generale quali la parità delle armi e i diritti di difesa.

Oltretutto, è interessante notare come la Corte sottolinei che a operare in questo contesto debbano essere gli agenti dello Stato o i privati cittadini che, però, si muovano su indicazione e sotto il controllo dei primi. Al contrario, nell'ipotesi in cui ad agire sia un privato in via autonoma, si fuoriesce dallo schema classico di *entrapment*. Sicché le pur possibili doglianze andranno esaminate sulla base delle norme generali in materia di acquisizione della prova e non nella prospettiva della provocazione [24].

Volgendo nuovamente lo sguardo alla *cyber deception*, risulta inevitabile domandarsi se essa costituisca o meno una forma di *entrapment*. Invero, la strategia è espressamente pensata per "attrarre" l'attaccante e, quindi, far sì che quest'ultimo sia in qualche modo "indirizzato" a colpire quel punto dell'infrastruttura: così intesa, essa entrerebbe in tensione con il criterio materiale.

In realtà, si sostiene che le tecniche decettive funzionino in modo essenzialmente "passivo" [25], in quanto non sarebbero idonee a esercitare un'influenza tale da istigare un soggetto a commettere un reato che altrimenti non avrebbe compiuto. Piuttosto, atteso anche l'elevato grado di competenze tecniche e la specificità di determinate condotte richieste per condurre azioni di accesso illecite a sistemi informatici, la *cyber deception* verrebbe in gioco solo a fronte di un proposito criminoso già determinato, rispetto al quale emerge l'esigenza di assicurare l'accertamento e di raccoglierne le prove [26]. In questa prospettiva, le

---

[24] Corte EDU, dec., 6 aprile 2024, *Shannon c. Regno Unito*.

[25] I. REID-A. OKEKE-RAMOS-M. SERAFIN, *Exploring the ethics of cyber deception technologies for defensive cyber deception*, in P. BEDNAR-J. KÄVRESTAD-E. BERGSTRÖM-M. RAJANEN-H.V. HULT-A.M. BRACCINI-A.S. ISLIND-F. ZAGHLOUL (a cura di), *Proceedings of the 10th International Conference on Socio-Technical Perspectives in Information Systems (STPIS 2024)*, 2024, p. 142.

[26] In senso analogo, sebbene in relazione agli *honeypot*, D. FRAUNHOLZ-S. DUQUE ANTON-C. LIPPS-D. RETI-D. KROHMER-F. POHL-M. TAMMEN-H.D. SCHOTTEN, *Demystifying deception technology: A survey*, in *arXiv:1804.06196*, 2018, p. 14; D. FRAUNHOLZ-C. LIPPS-M. ZIMMERMANN-S. DUQUE ANTON-J.K.M. MUELLER-H.D. SCHOTTEN, *Deception in Information Security: Legal Considerations in the Context of German and European Law*, in K. ADI-S. BOURDEAU-C. DURAND-V. VIET TRIEM TONG-A. DULIPOVICI-Y. KERMARREC-J. GARCIA-ALFARO (a cura di), *Foundations and Practice of Security*, Springer, 2025, p. 265, ove si osserva quanto segue: «*A criminal abusing a honeypot had the criminal intention before. The criminal actively searched for vulnerable systems and exploited the identified vulnerability to take advantage of the honeypot*». Così anche L. SPITZNER, *The Honeynet Project: trapping the hackers*, in *IEEE Security & Privacy*, 2003, vol. 1, n. 2, p. 17; R.N. GIRARD, *The Honeypot Stings Back: Entrapment in the Age of Cybercrime and a Proposed Pathway Forward*, in *Chicago Journal of International Law*, 2023, vol. 24, n. 1, pp. 190-191. Sempre in questa accezione, è utile rammentare che la

misure decettive potrebbero trovare un addentellato proprio nell'impalcatura edificata dai giudici di Strasburgo, sulla base della quale definirne i confini operativi.

Eppure, non può aprioristicamente escludersi che le caratteristiche dell'ambiente cibernetico fittizio finiscano per esercitare una qualche influenza sull'attaccante, magari determinando un ampliamento o aggravamento della sua manovra di azione. Del resto, attesa l'estrema duttilità degli strumenti in parola, configurabili in molteplici forme e a seconda delle esigenze del caso di specie, appare difficile poterli sussumere in uno *standard* unico [27].

5. Il modello delle *undercover operations*

Limitando l'orizzonte di analisi al contesto del procedimento penale e alla luce delle considerazioni finora svolte, può risultare utile, nel tentativo di proseguire il ragionamento, soffermarsi sull'istituto delle *undercover operations*, che – almeno sotto alcuni profili – sembra rievocare problematiche simili a quelle affiorate.

In via del tutto preliminare, giova rammentare come il dibattito sull'agente provocatore abbia conosciuto grande rilevanza anche nell'ordinamento interno [28], andando poi incontro a una sorta di metamorfosi con l'avvento della codificazione dei primi modelli di agente sotto copertura.

A partire dagli anni '90, infatti, il legislatore ha via via introdotto disposizioni speciali tese a consentire strumenti di indagine eccezionali in relazione a specifiche cerchie di reati, in seguito andatesi sempre più a estendere [29]. Ciò ha

giurisprudenza nazionale ritiene legittime le attività sotto copertura della polizia giudiziaria là dove l'azione dell'agente provocatore si limiti a «disvelare un'intenzione criminale esistente, ma allo stato latente, fornendo solo l'occasione per concretizzare la stessa e, quindi, senza determinarla in modo essenziale», così Cass., sez. III, 7 febbraio 2014, n. 20238.

[27] Simili criticità vengono rilevate anche da I. REID-A. OKEKE-RAMOS-M. SERAFIN, *Exploring the ethics of cyber deception technologies for defensive cyber deception*, cit., p. 142.

[28] Per una ricostruzione dell'evoluzione della figura di "agente provocatore" e dei principali orientamenti emersi in dottrina si vedano, *ex multis*, R. DELL'ANDRO, *Agente provocatore*, in *Enc. dir.*, vol. I., 1958, pp. 864-870; A. MALINVERNI, *Agente provocatore*, in *Noviss. dig. it.*, I, Torino, 1975, p. 396 ss.; C. DE MAGLIE, *Premesse allo studio dell'agente provocatore*, in *Riv. it. dir. proc. pen.*, 1989, p. 217 ss.; EAD., *L'agente provocatore. Un'indagine dommatica e politico-criminale*, Milano, Giuffrè, 1991; L. GALLI, *La responsabilità penale dell'agente provocatore*, in *La giust. pen*., 1939, II, p. 792.

[29] Lo schema delle *undercover operations*, ampiamente sviluppatosi negli anni, trova il suo archetipo nel settore degli stupefacenti, con la disposizione di cui all'art. 97, d.P.R. 9 ottobre 1990, n. 309, nella sua originaria formulazione. In materia di antiriciclaggio e lotta al mercato

condotto a un quadro normativo frammentato e disomogeneo, che poco si confaceva alla delicatezza della questione, soprattutto considerato l'impatto sulla persona coinvolta e, quindi, la necessità di assicurare adeguate garanzie [30].

Solo più tardi, con l'art. 9, l. 16 marzo 2006, n. 146, vengono poste le fondamenta per una disciplina più sistematica, con l'introduzione di uno "statuto" unitario delle attività "sommerse" [31], più compiutamente realizzato con la successiva riforma di cui alla l. 13 agosto 2010, n. 136 [32].

Per gli aspetti che qui maggiormente rilevano, è interessante porre l'accento sulla commistione funzionale che da sempre caratterizza l'istituto. Sebbene l'art. 9 orienti tali pratiche poliziesche «al sol fine di acquisire gli elementi di prova» – espressione da cui si può inferire la necessità di una previa *notitia criminis* –, esse presentano un'«attitudine indiscutibilmente "preventiva" della metodica» [33]. E invero, l'impianto predisposto dalla disposizione, che resta sganciato dalla disciplina codicistica, presta il fianco a operazioni retrospettive di ricerca di fattispecie delittuose, piuttosto che limitarsi ad accertarle [34]. Pur considerato che, guardando alla *ratio* della norma, dovrebbero comunque restare escluse dal suo ambito di applicazione le attività meramente esplorative o proattive, si ritiene che simili metodi possano essere adoperati anche per

---

illecito di armi, tale modello ha trovato espressione nell'art. 12-*quater*, d.l. 8 giugno 1992, n. 306. Tra gli altri interventi, si rammentano le operazioni sotto copertura coniate in tema di pedopornografia e di terrorismo, realizzate rispettivamente dall'art. 14, l. 3 agosto 1998, n. 269, e dall'art. 4, d.l. 18 ottobre 2001, n. 374. Per una prima analisi, V. FANCHIOTTI, *Agente sotto copertura (dir. proc. pen.)*, in *Enc. dir., Annali*, vol. VIII, Giuffrè, Milano, 2015, p. 18. Più in generale, sulla eterogenea gemmazione delle *undercover operations*, si rimanda a P. TROISI, *Investigazioni dell'agente sotto copertura*, in A. SCALFATI (a cura di), *Pre-investigazioni (espedienti e mezzi)*, Giappichelli, Torino, 2020, p. 237 ss.; B. FRAGASSO, *Provocazione di polizia e responsabilità penale*, in *Riv. it. dir. proc. pen*., 2022, p. 707 ss.

[30] *Ex multis*, V. FANCHIOTTI, *Agente sotto copertura (dir. proc. pen.)*, cit., p. 19.

[31] P. TROISI, *Investigazioni dell'agente sotto copertura*, cit., p. 240; B. FRAGASSO, *Provocazione di polizia e responsabilità penale*, cit., p. 720. Deve rammentarsi, a comprensione del contesto, che la riforma di cui alla l. n. 146/2006 si iscriveva sulla scia della Convenzione delle Nazioni Unite contro il crimine transazionale del 2000 (c.d. Convenzione di Palermo). In proposito, cfr. E. ANDOLINA, *Le operazioni sotto copertura nei reati contro i beni culturali tra standard europei ed irrisolte criticità*, in *Proc. pen. giust*., 2023, 1, p. 206.

[32] P. TROISI, *Investigazioni dell'agente sotto copertura*, cit., p. 240. Sulle criticità insite nel modello costruito dall'art. 9, l. n. 146/2006 e sulle modifiche apportate dalla successiva l. n. 136/2010, si veda in modo più diffuso V. FANCHIOTTI, *Agente sotto copertura (dir. proc. pen.)*, cit. p. 21.

[33] P. TROISI, *Investigazioni dell'agente sotto copertura*, cit., p. 243.

[34] *Ibidem*. Così anche G. MELILLO, *Le operazioni sotto copertura nelle indagini relative a finalità di terrorismo*, in G. DI CHIARA (a cura di), *Il processo penale tra politiche della sicurezza e nuovi garantismi*, Giappichelli, Torino, 2003, p. 49; D. CURTOTTI, *Operazioni sotto copertura*, in R. BARTOLOMEO (a cura di), *Le associazioni di tipo mafioso*, Utet, Milano, 2015, p. 435.

«"formare" la notizia di reato, in presenza di elementi di "sospetto" non ancora idonei a generare l'obbligo d'iscrizione» e, quindi, in un momento in cui l'indagine non sia ancora formalizzata [35].

Nella prassi, proprio in ragione della natura delle particolari condotte consentite agli agenti sotto copertura, si assiste a un vertiginoso assottigliamento del confine tra il settore della sicurezza pubblica e quello proprio del processo penale, ulteriormente amplificato dalle interferenze con i servizi di *intelligence* [36].

In questo contesto, già di per sé complesso, si inseriscono le modifiche attuate dalla l. 9 ottobre 2023, n. 137, sul disposto dell'art. 9, l. n. 146/2006 [37], dirette a potenziare le investigazioni nello spazio *cyber* grazie all'introduzione, accanto al già vario catalogo, di ulteriori tecniche pensate per essere espletate *online*.

In particolare, per le fattispecie di reato con finalità di terrorismo o eversive, oltre a tutte le modalità di cui alla lett. *a*) [38], si prevede che la polizia giudiziaria, nel corso di specifiche operazioni e allo scopo di raccogliere elementi di prova, possa altresì: «introdu[rsi] all'interno di un sistema informatico o telematico, danneggia[re], deteriora[re], cancella[re], altera[re] o comunque interven[ire] su un sistema informatico o telematico ovvero su informazioni, dati e programmi in esso contenuti, attiva[re] identità, anche digitali, domini e spazi informatici comunque denominati, anche attraverso il trattamento di dati personali di terzi, ovvero assum[ere] il controllo o comunque […] avval[ersi] dell'altrui dominio e spazio informatico comunque denominato o compi[ere] attività prodromiche o strumentali» [39].

---

[35] P. TROISI, *Investigazioni dell'agente sotto copertura*, cit., p. 247.

[36] Sul tema, D. CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. giust*., 2018, 3, p. 435 ss.

[37] Per un'analisi delle novità apportate dalla l. n. 137/2023, P. BRONZO, *Le indagini undercover nel mondo digitale*, in *Pen. dir. proc*., 19 ottobre 2023; S. CIAMPI, *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*, in *Proc. pen. giust.,* 2024, 3, p. 723.

[38] Nel dettaglio, ai sensi dell'art. 9, comma 1, lett. *a*), l. n. 146/2006, non sono punibili gli ufficiali di polizia giudiziaria che, per alcune tipologie di reato, anche per interposta persona, «danno rifugio o comunque prestano assistenza agli associati, acquistano, ricevono, sostituiscono od occultano denaro o altra utilità, armi, documenti, sostanze stupefacenti o psicotrope, beni ovvero cose che sono oggetto, prodotto, profitto, prezzo o mezzo per commettere il reato o ne accettano l'offerta o la promessa o altrimenti ostacolano l'individuazione della loro provenienza o ne consentono l'impiego ovvero corrispondono denaro o altra utilità in esecuzione di un accordo illecito già concluso da altri, promettono o danno denaro o altra utilità richiesti da un pubblico ufficiale o da un incaricato di un pubblico servizio o sollecitati come prezzo della mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o per remunerarlo o compiono attività prodromiche e strumentali».

[39] Art. 9, comma 1, lett. *b*), come interpolato dall'art. 2-*bis*, comma 4, lett. *a*), n. 1, d.l. 10 agosto 2023, n. 150, convertito con modifiche dalla l. 9 ottobre 2023, n. 137.

Inoltre, alle già eterogenee tipologie di illecito disseminate nel comma 1 [40], sono stati aggiunti, alla lett. *b-ter*), i «reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale». Ferma restando la finalità di scopo, pure rispetto a tali ipotesi criminose gli ufficiali di polizia giudiziaria, o i loro interposti, possono – attesa l'espressa previsione di non punibilità – dar seguito sia alle condotte "più tradizionali" di cui alla lett. *a*), sia a quelle digitali appena descritte [41].

Non da ultimo, la novella del 2023 incide sui poteri di impulso e di coordinamento conferiti al procuratore nazionale antimafia e antiterrorismo, attraverso l'estensione dei doveri di comunicazione previsti dai commi 4 e 8, art. 9, l. n. 146/2006, in ordine alle ipotesi di cui agli artt. 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*, c.p.p., facendovi così rientrare altresì i procedimenti riguardanti taluni gravi delitti di criminalità informatica [42].

Per quanto normativamente configurate, sotto l'ombrello delle operazioni sotto copertura ricade una cerchia indefinita di strumenti potenzialmente lesivi delle garanzie individuali, ancor più in ragione della svolta *cyber*. Non pare allora potersi escludere che, all'interno di questo incerto perimetro, vi ricada anche la *cyber deception*, intesa come azione di intervento dell'agente su un'infrastruttura di altri, avvalendosi della manipolazione controllata dell'ambiente digitale quale strumento investigativo. Se si ritenesse di condividere tale strada, l'attività decettiva svolta dalla polizia giudiziaria (o da interposte persone) a fini di indagine, per quanto "speciale", andrebbe ricondotta entro lo schema procedimentale individuato dall'art. 9, che assicura il rispetto di uno statuto minimo

---

[40] Il catalogo di cui alla lett. *a*) copre le fattispecie di reato di cui agli artt. 317, 318, 319, 319-*bis*, 319-*ter*, 319-*quater*, comma 1, 320, 321, 322, 322-*bis*, 346-*bis*, 353, 353-*bis*, 452-*bis*, 452-*ter*, 452-*quater*, 452-*sexies*, 452-*quaterdecies*, 453, 454, 455, 460, 461, 473, 474, 517-*quater*, 629, 630, 644, 648-*bis* e 648-*ter*, c.p. A questi si aggiungono i delitti concernenti armi, munizioni, esplosivi, nonché i delitti di cui: all'art. 12, commi 1, 3, 3-*bis* e 3-*ter*, d.lgs. 25 luglio 1998, n. 286; agli artt. 255-*bis*, 255-*ter*, 256, commi 1, secondo periodo, 1-*bis*, 3 e 3-*bis*, 256-*bis* e 259, d.lgs. 3 aprile 2006, n. 152; al d.P.R. 9 ottobre 1990, n. 309; e all'art. 3, l. 20 febbraio 1958, n. 75. Alle successive lett. *b*) e *b-bis*), vengono richiamati i delitti commessi con finalità di terrorismo o di eversione e i delitti *ex* artt. 518-*sexies* e 518-*septies* c.p.

[41] La lett. *b-ter*) dell'art. 9, comma 1, è stata aggiunta dall'art. 2-*bis*, comma 4, lett. *a*), n. 2, del già citato d.l. n. 150/2023, convertito con modifiche dalla l. n. 137/2023.

[42] S. CIAMPI, *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*, cit., p. 728-729. L'A. evidenzia come tale operazione si inserisca in una «più ampia manovra di convergenza» sul procuratore nazionale antimafia e antiterrorismo che investe istituti eterogenei», inclusi i rapporti con l'*ACN*. Con riferimento al rafforzamento delle prerogative della Procura nazionale antimafia e antiterrorismo, A. CISTERNA, *Il contrasto al terrorismo online e la tutela delle infrastrutture informatiche*, in *Dir. pen. proc.*, 2023, p. 1443.

di garanzie, benché non privo di importanti criticità.

In proposito, è sufficiente ricordare che il potere di disporre siffatte operazioni è rimesso agli organi di vertice o, su loro delega, ai responsabili di livello almeno provinciale, con obblighi informativi nei confronti dell'autorità giudiziaria sia prima dell'inizio delle operazioni che *in itinere*. Manca, tuttavia, una «disciplina dinamica dell'investigazione»: al di là dell'indicazione dei reati, non vi è traccia di condizioni di azionabilità e di forme di documentazione, né si impongono previe valutazioni sulla «necessità o indispensabilità» dell'operazione ovvero sulla «proporzionalità rispetto alle prerogative lese» [43].

Peraltro, a mente di quanto anzidetto sugli scivolosi confini tra prevenzione e repressione, è evidente come per le pratiche *online* tale demarcazione finisca ulteriormente per affievolirsi: ad aprire la strada a distorsioni applicative è, infatti, proprio la natura del contesto digitale e della fluidità delle condotte ivi realizzate [44], con la conseguenza che l'indagine potrebbe farsi occasione per intercettare indicazioni su crimini futuri o per testare la propensione a delinquere del soggetto-bersaglio [45].

Non da ultimo, le diverse declinazioni del contegno assunto dall'operatore creano «un'insidiosa quanto difficilmente eliminabile area di sovrapposizione fra agente infiltrato e agente provocatore» [46].

In definitiva, è evidente come tali tecniche generino profili di potenziale attrito con i canoni del giusto processo e del diritto di difesa, nonché, ancor prima, con il principio di legalità [47], a fronte di un corredo di garanzie, giusto quello imbastito dall'art. 9, che invece resta piuttosto flebile.

---

[43] P. TROISI, *Investigazioni dell'agente sotto copertura*, cit., p. 252.

[44] In altre parole, deve rilevarsi il «netto cambio di passo della cultura investigativa» che, proprio sulla spinta «della capacità intrusiva e della straordinaria "plasticità" degli strumenti messi a disposizione dall'informatica, è andata vieppiù abbracciando istanze preventive tutte imperniate su un controllo diffuso e generalizzato delle informazioni che possano essere ritenute utili a difendere la sicurezza dello Stato e della collettività da ogni minaccia o aggressione criminale o terroristica»; così, sebbene con più preciso riferimento al contesto della lotta al terrorismo, B. GALGANI, *Giudizio penale*, habeas data *e garanzie fondamentali*, in *Arch. pen.*, 2019, pp. 13-14.

[45] P. BRONZO, *Le indagini undercover nel mondo digitale*, cit., p. 6.

[46] S. CIAMPI, *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*, cit., p. 726. A evidenziare «l'insufficienza descrittiva» dell'agente sotto copertura, seppur nel più specifico contesto dei reati contro la pubblica amministrazione, è anche F.R. DINACCI, *L'agente sotto copertura e reati contro la pubblica amministrazione: nuovi difetti e vecchi vizi*, in *Arch. pen*., 2020, 4, p. 4 ss.

[47] *Ibidem*. Cfr. altresì E. ANDOLINA, *op. cit.,* p. 207.

6. Il ruolo dei soggetti privati: quali prospettive?

Finora l'analisi ha assunto una precisa prospettiva: quella di vagliare la possibilità di far ricorso alla *cyber deception* come strumento investigativo adoperato dalle autorità, seppur con le criticità esposte.

Del tutto diverso, invece, è lo scenario che si dischiude se a impostare e governare gli strumenti decettivi è il soggetto privato che li applica direttamente alla propria infrastruttura onde assicurarne il miglior livello di difesa da minacce informatiche.

Si è detto, infatti, come la *cyber deception* si presti in modo ottimale alle finalità di sicurezza della rete. Essa permette una protezione attiva dei sistemi, che si adatta alle contingenze e che, in ottica futura, è in grado di aggiornarsi e migliorarsi sulla base delle informazioni incamerate.

Del resto, sono gli stessi legislatori, unionale e nazionale, a richiedere *standard* sempre più elevati. Ne è un esempio l'art. 21, par. 1, dir. *NIS2*, là dove impone agli Stati di assicurare che i soggetti essenziali e importanti adottino «misure tecniche, operative e organizzative adeguate e proporzionate» per gestire i rischi di sicurezza, nonché per «prevenire o ridurre al minimo l'impatto degli incidenti» [48]. Ancora, ai sensi del secondo periodo della medesima disposizione, si precisa che l'adeguatezza, da parametrarsi al rischio esistente, deve tenere conto «delle conoscenze più aggiornate in materia» [49].

In via del tutto analoga, nel d.lgs. n. 138/2024, di recepimento della richiamata direttiva, l'art. 24 rivolge il medesimo obbligo direttamente ai soggetti essenziali e a quelli importanti, che sono dunque tenuti a porre in essere tutti gli accorgimenti necessari a garantire la protezione della propria infrastruttura. Anche in questo caso, il test di adeguatezza non può non considerare gli sviluppi in termini di *expertise* e stato dell'arte, sì da incoraggiare misure al passo con l'evoluzione tecnologica e le *best practices* di settore.

Nella prassi, dunque, quel che accade è che i privati, in ragione tanto degli interessi economici sottesi quanto degli obblighi di *compliance*, sviluppino

---

[48] Per "incidente" deve intendersi «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi»; così art. 2, comma 1, lett. *t*), d.lgs. n. 138/2024.

[49] Sugli obblighi imposti dalla dir. *NIS2* e sulla relativa implementazione nel sistema interno, *ex multis*, I. DEMURO, *La Governance della Cybersecurity secondo la Direttiva NIS*, in *Le Società*, n. 8-9, 2025, p. 881 ss.; L. PREVITI, *La nuova legge sulla cybersicurezza, un passo avanti e due indietro*, in *Gior. dir. amm*., 2025, n. 1, p. 60 ss. Inoltre, nell'ottica di rafforzare il livello complessivo di sicurezza, deve sottolinearsi il ruolo chiave delle politiche di *coordinated vulnerability disclosure*, di cui all'art. 12, dir. *NIS2*. Sul tema, F.N. RICOTTA, *Vulnerability disclosure e penetration testing: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2*, in *Riv. it. inf. dir.*, 2024, pp. 81-92.

strategie di cybersicurezza all'avanguardia, tra cui senz'altro può ricomprendersi la *cyber deception*.

Per altro verso, non ci si può esimere dal rilevare come l'art. 25, d.lgs. n. 138/2024, nel far eco all'art. 23, dir. *NIS2*, obbliga i soggetti essenziali e importanti a notificare al *CSIRT Italia*, senza ingiustificato ritardo, gli incidenti significativi [50], prefigurando altresì, qualora si sospetti che l'evento abbia carattere criminale, il coinvolgimento del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione [51].

Il successivo art. 26, poi, estende, su base volontaria, la segnalazione anche agli incidenti diversi da quelli per cui è previsto l'obbligo, alle minacce informatiche e ai quasi-incidenti [52], a cui si applica il medesimo modello procedurale.

Accanto a questi canali, trova spazio una serie di disposizioni in tema di monitoraggio, vigilanza ed esecuzione (si pensi, in particolare, agli artt. 34, sui poteri riconosciuti all'autorità nazionale competente *NIS*, e 36, sulle ispezioni individuali) e, più in generale, di supporto ai soggetti coinvolti. Nel complesso, si va così creando uno stretto reticolato di collaborazione tra i privati e le autorità pubbliche che, però, si configura sotto plurime vesti, alcune piuttosto informali, non andando esente da alcune criticità [53].

Questa rinvigorita cooperazione – che, d'altronde, si è fatta strada con sempre maggiore insistenza nei più disparati settori (si pensi, ad esempio, all'antiriciclaggio e all'antimafia) – presenta aspetti positivi. La condivisione di indicatori

---

[50] Nel dettaglio, il sistema di notifica si basa su una "pre-notifica", da inviare al più tardi entro 24 ore dall'evento, in cui si dia già atto, ove possibile, se l'incidente «possa ritenersi il risultato di atti illegittimi o malevoli» o se «può avere un impatto transfrontaliero» (art. 25, d.lgs. n. 138/2024, comma 5, lett. *a*)). Segue, nel termine di 72 ore, una "notifica" di aggiornamento comprensiva di una valutazione iniziale dell'accaduto (lett. *b*)). Ancora, entro un mese dall'evento, deve essere presentata una più dettagliata "relazione finale" (lett. *d*)), preceduta, solo se richiesta dal *CSIRT* Italia, da una "relazione intermedia" (lett. *c*)). Per i casi in cui l'incidente sia ancora in corso all'atto della relazione di cui alla lett. *d*), si richiede che si continui a inviare una relazione mensile, nonché una conclusiva a un mese dalla chiusura della gestione dell'incidente (lett. *e*)). Ai sensi del comma 4, un incidente si definisce "significativo" là dove: «a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli».

[51] Art. 25, d.lgs. n. 138/2024, comma 8.

[52] Si tratta dei c.d. "*near-miss*", ossia «un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato», inclusi i casi in cui sia efficacemente evitato; così art. 2, comma 1, lett. *u*), d.lgs. n. 138/2024.

[53] Per un'approfondita disamina dell'evoluzione del fenomeno delle *public-private partnerships*, si veda G. LASAGNI, *Public-private cooperation in the detection and investigation of criminal offences in Italy*, in B. VOGEL-E. KOSTA-M. LASSALLE (a cura di), *Law of public-private cooperation against financial crime*, Intersentia, Cambridge, 2025, p. 245 ss.

di rischio (c.d. *compliance* PPP [54]) e, quindi, di dati informativi non individualizzati, ma utili ad analizzare le vulnerabilità e comprendere meglio la fenomenologia criminosa, può senz'altro contribuire, ad esempio, a rafforzare la resilienza complessiva del sistema e supportare le autorità di contrasto nel definire le linee di prevenzione e repressione.

D'altro canto, però, i meccanismi di *partnership*, se adoperati in chiave investigativa, aprono a molteplici zone d'ombra [55].

Al di là dei casi – forse meno problematici, ma non più troppo rispondenti allo scenario attuale – in cui l'interazione tra la parte pubblica e quella privata si esaurisca con la raccolta della *notitia criminis*, i rischi sono oggi messi in evidenza proprio dai rinnovati compiti di monitoraggio e vigilanza sugli obblighi di *cybersecurity*. Rispetto a questi, infatti, viene riconosciuto un ampio e non definito novero di poteri in capo all'*ACN*, nonché alla sua articolazione *CSIRT Italia*, tali da favorire una considerevole collaborazione in una dimensione preventiva, da cui, però, può discendere una certa circolazione informativa. Il problema, allora, diviene evidente, posto che una commistione di questo tipo produce una pericolosa osmosi tra ambito preventivo e investigativo, a scapito del principio generale di separazione tra il processo penale e altri tipi di accertamento [56].

Le medesime problematiche, lo si sarà intuito, fanno da cornice ai casi di impiego di strategie di difesa da parte del soggetto privato. È del tutto comprensibile, infatti, che quest'ultimo, nell'ottica di assicurare la *compliance* rispetto agli obblighi in materia di cybersicurezza, faccia ricorso alle misure tecniche più idonee, tra cui – per l'appunto – anche quelle decettive. Il problema, però, è che la *cyber deception* non lascia indifferenti in termini di compendio conoscitivo che è in grado di conseguire, al punto da poter essere fagocitata nell'orbita di interesse delle dinamiche di collaborazione con il pubblico.

Tralasciando il caso in cui a venire in rilievo siano solo informazioni di contesto e non individualizzate, una prima ipotesi, quasi fisiologica, è che il privato, a seguito del rilevamento effettuato per il tramite della *cyber deception*, dia notizia dell'attività intrusiva al pubblico ministero o alla polizia giudiziaria, mediante denuncia – da poter corredare con il *report* dell'attività decettiva e, dunque, con i dati ad essa relativi –, da cui potrebbe scaturire l'avvio di un procedimento penale.

---

[54] Sulla nozione di *Public Private Partnership* (PPP), nelle due diverse accezioni di *compliance* e *investigative*, nonché sulle relative caratteristiche, si veda G. LASAGNI, *Public private partnerships nell'antiriciclaggio e antiterrorismo: una nuova forma di outsourcing del processo penale?*, in *Dir. pen. com. – Riv. trim.*, 2021, 3, pp. 153-160.

[55] *Ivi*, p. 163.

[56] Su questi temi, si rinvia alle riflessioni di A. PUGLIESE-G. LASAGNI, *Cybersecurity, indagini amministrative, cooperazione pubblico-privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa*, in questo volume.

Del tutto differente e certamente più preoccupante è, invece, lo scenario che si profila nel caso in cui la *cyber deception* si inserisca in contesti di vere e proprie *investigative* PPP: il rischio è che le autorità pubbliche, in ragione della disponibilità tecnica del privato, ma anche dei meno stringenti margini di manovra, finiscano per "incoraggiare" determinate attività di controllo con riferimento a specifiche casistiche. Si tratta di una possibile torsione applicativa che diviene ancor più insidiosa se si pensa che essa non opererebbe in una fase postuma, quando l'azione criminosa si è già compiuta, ma financhè la precederebbe: in altre parole, l'attività decettiva di difesa del privato verrebbe in una certa misura strumentalizzata. Il risultato, per quanto voluto o meno, appare chiaro: giungere a contenuti conoscitivi fuori dagli schemi procedimentali, eludendo le garanzie che dovrebbero assistere la raccolta di informazioni in contesti di accertamento tanto amministrativo quanto – ancor di più – penale.

Con questo, però, non si vuole disconoscere *in toto* l'apporto che i soggetti privati sono in grado di offrire rispetto alle finalità di contrasto alla criminalità; piuttosto, proprio alla luce del ruolo sempre più centrale che vanno ritagliandosi, quel che si auspica è una riflessione più attenta sui meccanismi collaborativi che si instaurano con le autorità pubbliche, onde evitare che, dietro i più nobili intenti, si annidino intollerabili prassi ambigue di procacciamento di elementi conoscitivi da destinare alla sede penale, sottratte ai necessari presidi procedimentali.

7. Alcune considerazioni (non) conclusive

Provando a trarre le fila degli spunti di riflessione abbozzati, quel che certamente emerge è la propensione a cercare delle innovative forme di contrasto alla criminalità, più attagliate al mutato contesto sociale in cui l'ambiente digitale occupa uno spazio sempre maggiore, per non dire preponderante. La spinta tecnologica, dunque, è una conseguenza quasi obbligata, senza la quale non sarebbe possibile agire sulle nuove fenomenologie criminose.

A fronte di tecniche sempre più sofisticate, che richiedono non solo un compendio di conoscenze adeguate, ma altresì la disponibilità di risorse e strumenti per svilupparle, il rischio è quello di avviarsi verso una progressiva "esternalizzazione" dell'attività investigativa anche in ambito *cyber*, come già avvenuto nei settori della lotta al terrorismo, al riciclaggio e alla mafia.

Quanto finora detto, però, non esaurisce il novero delle questioni poste dalla *cyber deception*. Una delle proprietà della strategia in parola – che, peraltro, la rende uno strumento così appetibile per le autorità di contrasto – è quella di inserirsi nella dinamica dell'azione delittuosa e di raccogliere delle informazioni

a essa inerenti, tra cui tendenzialmente anche dati identificativi, quali l'indirizzo IP [57]. Di qui, la necessità di garantire che il trattamento di tali elementi avvenga in conformità con il quadro normativo in materia di *data protection*: in linea di massima, dunque, esso dovrà iscriversi entro i limiti imposti dalle finalità legittime e la conservazione non potrà eccedere quanto necessario agli scopi per cui viene effettuata la raccolta, oltre a rispettare gli ulteriori principi di liceità, correttezza e trasparenza del trattamento, esattezza e minimizzazione dei dati, integrità e riservatezza.

Vi è di più. L'impiego della *cyber deception* da parte di autorità pubbliche a fini penali induce a interrogarsi anche sul grado di invasività dello strumento in parola, soprattutto attesa la sua capacità di raccogliere dati di carattere personale. In realtà, nel caso di specie, molto dipende dalla tecnica attuata, dai livelli di interazione e, quindi, dalla tipologia delle informazioni captabili. Vero è che tendenzialmente a essere intercettato sarebbe il "solo" indirizzo IP, ma le operazioni devono comunque iscriversi entro le indicazioni ricavabili dalla dir. (UE) 2016/680 e, più in generale, dagli artt. 8 CEDU e 7 e 8 Carta di Nizza, come interpretati dalla relativa giurisprudenza convenzionale e unionale [58].

Peraltro, pur non potendo approfondire la questione in questa sede, è fondamentale evidenziare che strumenti di *cyber deception* andrebbero altresì valutati alla luce dell'*AI Act*, per vagliare quali possano essere i livelli di rischio a essi legati e da cui potrebbero discendere specifici obblighi normativi.

Sotto altra accezione, si è detto che la *cyber deception* produce, in ultima istanza, un *report* che registra la sequenza degli avvenimenti e le informazioni relative all'evento. Si tratta, però, di un documento che potremmo dire "preconfezionato", rispetto alla cui formazione pare difficile poter interagire. Ne deriva che, ai fini di salvaguardarne la spendibilità processuale, è necessario se non altro garantirne la verificabilità. L'orizzonte entro cui muoversi, perciò, non può che essere quello di assicurare che le parti siano in grado di esercitare tutte le prerogative attraverso cui si esplica il principio del contraddittorio, in condizioni di parità delle armi.

---

[57] In proposito, cfr. D. FRAUNHOLZ-C. LIPPS-M. ZIMMERMANN-S. DUQUE ANTON-J.K.M. MUELLER-H.D. SCHOTTEN, *Deception in Information Security: Legal Considerations in the Context of German and European Law*, cit., 271.

[58] Per una prospettiva sui contenuti della direttiva e per un'analisi critica, cfr. B. GALGANI, *Giudizio penale,* habeas data *e garanzie fondamentali*, cit., p. 8 ss. In relazione al caso della *cyber deception*, deve segnalarsi che alcuni studiosi hanno dubitato di poter considerare gli indirizzi IP alla stregua di dati personali, poiché gli stessi sono collegati a dei *devices* che, a loro volta, contribuiscono a identificare – spesso grazie anche agli ulteriori elementi raccolti – l'*user*. Nell'ipotesi degli *honeypot*, però, ciò viene messo in discussione dal fatto che l'identificazione della persona fisica non sarebbe possibile con gli strumenti a disposizione dell'operatore. Così P. SOKOL-J. MÍŠEK-M. HUSÁK, *Honeypots and honeynets: issues of privacy*, in *EURASIP Journal on Information Security*, 2017, 4, p. 6.

Certamente è quanto mai opportuno, anzi doveroso, che gli operatori si attengano, sia nella predisposizione delle strategie di difesa, dunque delle tecniche decettive, sia all'atto di eventuali incidenti, alle *best practices* e agli *standard* di settore. Ugualmente, la raccolta di elementi informativi inerenti all'attacco e a chi lo ha perpetrato deve avvenire conformemente ai criteri di *digital forensics*, per assicurare la qualità dei dati ottenuti, ma anche la possibilità di verificare – e, se del caso, questionare – il corretto svolgimento delle operazioni effettuate.

Ciò, però, non risolve comunque la questione a monte sull'utilizzabilità degli elementi in parola, che non può essere affrontata in modo omnicomprensivo, ma necessita di una più attenta disamina a seconda delle specifiche vesti che si assegnano alla *cyber deception*.

In conclusione, resta una considerazione di fondo: le potenzialità delle tecniche decettive stanno ridisegnando gli schemi e le strategie di cybersicurezza. A cambiare è il paradigma. La *cybersecurity*, che fa dell'autenticità e dell'integrità due elementi essenziali, si apre ora all'opportunità di inglobare misure ingannevoli che, attraverso la messa a punto di dati, sistemi o reti fittizie, mirano a proteggere gli omologhi originali.

Il paradosso, però, è ulteriore. Se si cambia la prospettiva di analisi, è ben evidente che simili attività "d'inganno" possano essere impiegate anche dai soggetti che, a diverso titolo, potrebbero essere destinatari dell'azione intrusiva operata dalle autorità pubbliche. Si pensi, in particolare, a strumenti investigativi tecnologici adoperati dagli inquirenti che finiscano per essere sviati proprio dalla *deception*, con l'ulteriore eventualità che i dati restituiti siano quelli fittizi.

Resta centrale, dunque, promuovere la cultura del dato e favorire lo sviluppo di *best practices*, in modo da accrescere la resilienza complessiva dell'ecosistema digitale ed evitare che strumenti pensati per la sua difesa possano finire, da ultimo, per comprometterla.

Parte III

Cybersicurezza e tutela dei diritti fondamentali: una prospettiva critica

Capitolo 11

Polizia, *big data* e società digitale: sicurezza dei dati, sicurezza dai dati [*]

Giulia Fabini [**]

Abstract: La sicurezza dei dati non è l'unica forma di protezione cui occorre prestare attenzione quando si affronta il delicato tema dell'impiego dei *big data* e delle tecnologie digitali da parte della polizia. Esiste, infatti, una questione ancora più complessa: quella della sicurezza dai dati. Con questa espressione si intende fare riferimento ai rischi cui vengono esposti gli individui a causa di un uso improprio o distorto delle informazioni da parte delle agenzie del controllo istituzionale, nelle fasi di raccolta, analisi e conservazione dei dati. Adottando una prospettiva di criminologia critica digitale, il capitolo analizza il fenomeno della polizia predittiva e riflette sul ruolo dei *big data* e dei software di analisi algoritmica nella costruzione della conoscenza del reale. Le conclusioni offrono alcune riflessioni sull'apporto che la nascente criminologia critica, in dialogo con discipline quali l'informatica giuridica, la sociologia del diritto e la procedura penale, può fornire alla discussione sui rischi che tali tecniche pongono ai diritti individuali, ipotizzando possibili direzioni cui guardare per il loro superamento. Ciò che è in gioco sono i meccanismi di produzione della conoscenza di un dato fenomeno, di elaborazione della soluzione rispetto all'interpretazione che si dà di tale fenomeno e di individuazione della responsabilità nel meccanismo decisionale.

Keywords: Big data – Società digitale – Criminologia digitale – Polizia predittiva – Sicurezza dai dati

---

[*] Il presente capitolo riprende alcune delle argomentazioni e delle tematiche trattate nel testo di prossima pubblicazione *Il Controllo Data-Driven: la natura tecnosociale della (cyber)sicurezza*, pubblicato dalla scrivente e in uscita per Bononia University Press. Il libro è un risultato delle ricerche condotte dall'autrice nell'ambito del progetto EcoCyber per il paternariato esteso SERICS.

[**] Ricercatrice a tempo determinato di tipo a) in sociologia del diritto e della devianza (SPS/12), presso Dipartimento di Scienze Giuridiche, Università di Bologna, giulia.fabini@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

La raccolta, l'elaborazione e l'analisi delle informazioni costituiscono oggi l'ossatura delle strategie orientate ad anticipare i comportamenti criminali, garantire l'identificazione dei colpevoli e sorvegliare i potenziali autori di reato.

Nella società datificata, le informazioni personali diventano una risorsa cruciale: esse devono essere acquisite e utilizzate per finalità di sicurezza, ma, al contempo, necessitano di una rigorosa protezione contro accessi non autorizzati e usi impropri. Da questo duplice imperativo nasce una tensione strutturale per le agenzie del controllo, specialmente per le forze di polizia: da un lato, esse raccolgono, analizzano e conservano informazioni su individui e gruppi per finalità di controllo, sorveglianza e indagine; dall'altro, devono proteggere questi stessi dati. Tale compito non è tuttavia sempre facile e gli episodi di *data breach* non sono poi così rari.

Un esempio recente e particolarmente rilevante in contesto italiano è l'inchiesta giudiziaria sul cosiddetto 'caso dossieraggio', esplosa a Milano nel 2024. Secondo l'accusa, un gruppo organizzato composto da ex appartenenti alle forze dell'ordine, consulenti informatici e investigatori privati avrebbe effettuato accessi abusivi ad alcune banche dati [1], tra le quali lo SDI (circa 350.000 accessi), sottraendo dati personali e investigativi allo scopo di produrre e rivendere dossier su vari soggetti. Lo SDI, Sistema di indagine gestito dal Ministero dell'Interno – Dipartimento della Pubblica Sicurezza, costituisce la principale banca dati interforze italiana. Esso consente la raccolta, l'elaborazione e la condivisione di informazioni tra le diverse forze di polizia – tra cui Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza – per finalità di prevenzione e repressione dei reati. Lo SDI integra dati provenienti da banche dati nazionali (anagrafi, veicoli, armi, precedenti giudiziari) e da sistemi europei come il SIS II (*Schengen Information System*). L'accesso è consentito esclusivamente a operatori autorizzati, secondo livelli differenziati di autorizzazione, e tracciato nel rispetto della disciplina sul trattamento dei dati personali per finalità di polizia, prevista dal d.lgs. n. 51/2018, attuativo della

[1] La banca dati dell'Inps, Serpico (Sistema informatico dell'Agenzia delle Entrate), Anpr (Anagrafe nazionale della popolazione residente), Siva (Sistema informativo valutario).

Direttiva (UE) 2016/680. Le indagini hanno ipotizzato l'estrazione di centinaia di migliaia di informazioni, con ricavi per diversi milioni di euro e il coinvolgimento di figure di alto profilo come magistrati, prefetti, manager e atleti di livello internazionale. Tra gli indagati figurano l'ex sovrintendente di polizia Carmine Gallo e l'informatico Nunzio Calamucci, mentre un ruolo di rilievo sarebbe stato svolto da società di copertura presentate come strutture di consulenza per celare la reale natura delle operazioni e la successiva commercializzazione delle informazioni. Va sottolineato che la ricostruzione finora disponibile è in divenire e le indagini sono ancora in corso. Inoltre, data la 'zona grigia' tra pratiche investigative lecite e condotte illecite (in particolare nelle investigazioni private o nelle attività di *intelligence*), la stessa definizione di dossieraggio è oggetto di discussione sia negli articoli giornalistici sia tra i protagonisti dell'inchiesta [2]. Tuttavia, il caso mostra con chiarezza come la stessa infrastruttura informativa che alimenta l'attività di polizia possa diventare vulnerabile se non è adeguatamente protetta da intrusioni interne ed esterne.

La sicurezza *dei* dati, quella di cui abbiamo sin qui trattato, non è l'unico tipo di protezione cui si dovrebbe prestare attenzione quando ci si confronta con il delicato tema dell'utilizzo dei *big data* e della tecnologia digitale da parte della polizia. Infatti, esiste il tema ancora più delicato della sicurezza *dai* dati. Con tale locuzione, facciamo riferimento ai rischi cui vengono sottoposti i soggetti in conseguenza di un utilizzo scorretto dei dati, dal momento della loro raccolta, alla loro analisi e conservazione. Ci riferiamo, ad esempio, ai rischi legati alla sorveglianza, alla violazione della *privacy*, agli effetti di razzializzazione di certi software, agli effetti di ridefinizione dei confini della cittadinanza e alla produzione di conoscenza parziale e viziata sulla realtà. Mentre la prima versione della sicurezza, sebbene perfettibile (come dimostrano i casi sopra esposti), riceve non poca attenzione dal punto di vista istituzionale e sempre più anche della ricerca, la seconda versione della sicurezza resta ancora marginale quando si parla di cybersicurezza e sistemi di controllo. Invece, è di questa, della sicurezza *dai* dati, che il presente capitolo si prefigge di parlare.

Il capitolo è così strutturato: nel secondo paragrafo, presentiamo la prospettiva di analisi entro cui si inserisce la trattazione, ovvero la criminologia

[2] Per la ricostruzione dei fatti, ci siamo basate su fonti giornalistiche. In particolare: *Inchiesta hacker: i dossieraggi, i clienti e le vittime. Cosa sappiamo finora*, in *Il Sole 24 Ore*, 30 ottobre 2024, https://www.ilsole24ore.com/art/inchiesta-hacker-dossieraggi-clienti-e-vittime-cosa-sappiamo-finora-AGwLwAo; *Inchiesta sui dati rubati: l'hacker ammette e spiega i ruoli*, in *Il Giorno*, 31 ottobre 2024, https://www.ilgiorno.it/milano/cronaca/inchiesta-dati-rubati-interrogatori-d3eh7xg4; *Tutto quello che c'è da sapere sul caso dossieraggio (che dossieraggio non è)*, in *Domani*, 28 ottobre 2024, https://www.editorialedomani.it/fatti/tutto-quello-che-ce-da-sapere-sul-caso-dossieraggio-che-dossieraggio-non-e-wslhkvxh.

digitale; nel terzo paragrafo forniamo una spiegazione dei *big data*: che cosa sono e che implicazioni hanno per la produzione di conoscenza sul fenomeno della criminalità e sull'elaborazione della reazione istituzionale alla stessa; nel quarto paragrafo, ci concentriamo sulla polizia predittiva come esempio di utilizzo dei *big data* e di tecnologia *data-driven* da parte delle agenzie del controllo; nel quinto paragrafo passiamo a una disamina dei rischi connessi all'utilizzo dei modelli di polizia predittiva. Nelle conclusioni, proponiamo alcune riflessioni sull'apporto che la nascente criminologia critica in dialogo con altre discipline, come l'informatica giuridica, la sociologia del diritto e la procedura penale, può offrire ai ragionamenti sui rischi che queste tecniche pongono ai diritti individuali, ipotizzando direzioni possibili a cui guardare per il loro superamento. Il dibattito critico criminologico sulle strategie di controllo e prevenzione del crimine nelle società digitali richiama l'attenzione non tanto sui rischi per la sicurezza dei dati, quanto su ulteriori rischi per la sicurezza dai dati. Ciò che è in gioco sono i meccanismi di produzione della conoscenza di un dato fenomeno, di elaborazione della soluzione rispetto all'interpretazione che si dà di tale fenomeno, e di individuazione della responsabilità nel meccanismo decisionale.

2. Criminologia digitale

Nelle società digitali, l'evoluzione tecnologica trasforma in profondità le forme della criminalità, nonché i meccanismi di controllo, prevenzione e sorveglianza, cosa su cui la criminologia – in particolare quella critica [3] – ha iniziato solo di recente a riflettere in maniera articolata, almeno a livello europeo, dando vita a un nuovo campo di studi, la criminologia digitale [4].

La criminologia digitale emerge dalla necessità di comprendere le trasformazioni della criminalità e del controllo nel contesto di una società digitale e si pone

[3] La criminologia critica analizza il crimine come risultato di definizioni legali e pratiche di controllo selettivo, interpretando entrambi come espressioni delle strutture di potere diseguali che attraversano la società. Si potrebbe affermare che essa non studia il controllo istituzionale come reazione al crimine, bensì il crimine come effetto del controllo istituzionale in una società intrinsecamente conflittuale e modellata da relazioni di potere. In questo senso, lo studio del crimine – e in particolare delle reazioni sociali al crimine (cioè il sistema penale) – diventa studio delle strutture di potere che governano l'organizzazione sociale. A. SBRACCIA, *Criminologie post-coloniale*, in C. RINALDI-P. SAITTA (a cura di), *Criminologie critiche contemporanee*, Milano, Giuffrè Francis Lefebvre, 2018, pp. 27-49.

[4] M. KAUFMANN-H. LOMELL, *De Gruyter Handbook of Digital Criminology*, Berlin, De Gruyter, 2025.

come un avanzamento teorico ed empirico rispetto allo studio del *cybercrime*. La società contemporanea è immersa in un ambiente iperconnesso, dove il digitale non è un 'altrove', ma si intreccia in modo costitutivo con le vite materiali, affettive, economiche e politiche delle persone. La criminologia digitale lascia dunque da parte il dibattito sulle definizioni di cybercrime, poiché la costante compresenza tra realtà online e offline che caratterizza le società digitali rende sempre più difficoltoso distinguere la 'cybercriminalità' dalla 'criminalità tradizionale' [5]. In tutto questo, il digitale non rappresenta più un oggetto di studio esterno o una 'nuova frontiera' per le teorie già esistenti, ma costituisce un elemento strutturale della realtà sociale contemporanea, che trasforma in profondità cosa intendiamo per crimine, chi è coinvolto nei processi di controllo e in che modo la giustizia viene esercitata. L'emergente criminologia digitale viene quindi concepita non come sottodisciplina tematica (limitata, per l'appunto, allo studio del cybercrime), ma come una prospettiva teorica che obbliga la criminologia a rivedere le proprie categorie fondative [6].

La criminologia digitale critica ha iniziato a interrogarsi sulla natura delle tecnologie digitali come attori sociali che partecipano attivamente alla costruzione della criminalità e del controllo. In questo contesto, le tecnologie non possono più essere considerate strumenti neutri, ma vanno intese come agenti attivi, capaci di modellare il comportamento, la percezione del rischio, le relazioni di potere e le stesse definizioni di devianza [7].

Esistono alcuni nuclei teorici della criminologia digitale. Uno di questi è l'*Actor-Network Theory* (ANT), o *teoria dell'attore-rete* [8]. L'ANT si fonda sull'idea che l'azione sociale non sia prodotta esclusivamente dagli esseri umani, ma da attori eterogenei, umani e non umani, che interagiscono all'interno di reti sociotecniche. Il potere, il sapere e l'azione sono quindi performati da configurazioni socio-materiali che includono, necessariamente, le tecnologie come coproduttrici degli esiti sociali dell'azione. L'azione, quindi, non è più frutto della

---

[5] A. Di Nicola, *Criminalità e criminologia nella società digitale*, Milano, FrancoAngeli, 2021. Di Nicola propone di collocare la criminalità lungo un *continuum*: a un estremo si trovano i reati pienamente tecnologici e virtuali, che non potrebbero esistere senza l'ambiente digitale; all'estremo opposto, crimini puramente fisici, privi di qualsiasi componente tecnologica. Tra questi poli si collocano una molteplicità di fenomeni ibridi, in cui la tecnologia assume un ruolo variabile – talvolta marginale, talvolta centrale – nella dinamica del comportamento criminale.

[6] A. Powel-G. Stratton-R. Cameron, *Digital criminology. Crime and justice in digital society*, Abingdon, Oxon, Routledge, 2018.

[7] S. Milivojevic, *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century*, Abingdon, New York, Routledge, 2021.

[8] B. Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford, Oxford University Press, 2005.

scelta (e, dunque, della responsabilità) esclusivamente umana, ma è sempre l'esito di azioni di *ibridi umano-macchina*.

Fondamentale è anche il concetto di *black box* [9], con cui ci si riferisce al fatto che le procedure che trasformano gli *input* in *output* funzionano come scatole nere, ovvero sono opache, impediscono di osservarne il funzionamento interno. In un contesto altamente digitalizzato, questo effetto di opacità – o 'impercepibilità' – diventa sempre più pervasivo: le tecnologie operano costantemente in *background*, modellano l'azione sociale, ma raramente diventano oggetto di analisi critica. Esisterebbe, infatti, una *technological unconscious* [10] che accompagna l'impatto della tecnologia nella vita sociale: la tecnologia c'è e produce degli effetti, ma ci dimentichiamo della sua esistenza, non siamo consapevoli del suo ruolo o non ne teniamo conto. La naturalizziamo. Proprio contro questa tendenza si collocano le riflessioni più recenti della criminologia digitale, che cercano di riportare al centro dell'analisi i processi sociotecnici che co-producono criminalità, controllo e giustizia, superando tanto le visioni che collocano l'umano al centro dei processi di trasformazione delle società contemporanee, quanto quelle che invece vedono tali trasformazioni come determinate dalla tecnologia.

Un altro concetto chiave che aiuta a comprendere le trasformazioni contemporanee del controllo sociale è quello di *ubiquitous surveillance*, ossia sorveglianza ubiqua. Questo concetto, elaborato inizialmente da David Lyon [11] e successivamente approfondito da Mark Andrejevic [12], rappresenta un'evoluzione dei paradigmi precedenti della sorveglianza: dal modello panottico [13], alla sorveglianza post-panottica [14], fino a una nuova forma di sorveglianza diffusa, pervasiva e continua. In questo quadro, la sorveglianza non è più esercitata solo da istituzioni verticali e visibili, ma è automatizzata, decentralizzata, volontaria e integrata nelle pratiche quotidiane della vita digitale. La sorveglianza diventa 'ubiqua' perché è ovunque e sempre attiva, resa possibile da ciò che Haggerty ed Ericson [15] definiscono *surveillance assemblage*: un insieme dinamico e

---

[9] B. LATOUR, *Science in Action: How to Follow Scientists and Engineers Through Society*, Cambridge (MA), Harvard University Press, 1987.

[10] S. MILIVOJEVIC, *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century*, cit.

[11] D. LYON, *Surveillance studies: An overview, Cambridge*, Polity Press, 2007.

[12] M. ANDREJEVIC, *Ubiquitous surveillance*, in K. BALL-K. HAGGERTY-D. LYON (eds), *The Routledge Handbook of Surveillance Studies*, Abingdon-Oxon, Routledge, 2012, pp. 91-98.

[13] M. FOUCAULT, *Sorvegliare e punire. Nascita della prigione*, Torino, Einaudi, 1976.

[14] Z. BAUMAN, *Liquid Modernity*, Cambridge, Polity, 2000.

[15] K. HAGGERTY-R. ERICSON, *The surveillant assemblage*, in *British Journal of Sociology*, 2000, vol. 4, pp. 605-622.

interconnesso di tecnologie, attori e dispositivi che aggregano dati sugli individui da fonti diverse (telefoni, carte di credito, videocamere, social media, dispositivi smart). In molti casi, i dati vengono raccolti senza piena consapevolezza, ma spesso anche con il consenso attivo degli utenti, che forniscono informazioni in cambio di servizi digitali, comodità o accesso a piattaforme. Inoltre, la sorveglianza ubiqua è oggi fortemente intrecciata con processi di privatizzazione e monetizzazione: i dati non sono solo strumenti di controllo, ma risorse economiche, vendute, scambiate e sfruttate da aziende private per profitto, con profonde implicazioni in termini di potere, disuguaglianza e giustizia sociale [16]. In questo contesto, la sorveglianza non è più solo un meccanismo repressivo ma una dimensione strutturale della vita nella società digitale, che pone interrogativi urgenti su *agency*, autonomia, *privacy* e governance algoritmica. La criminologia digitale, in quanto campo critico, è chiamata a interrogare questi dispositivi di potere e a comprendere come contribuiscano alla costruzione e alla gestione della devianza nel presente iperconnesso.

3. Cosa sono i *big data*

Secondo Sarah Brayne, una sociologa statunitense che ha studiato l'utilizzo dei *big data* da parte della polizia di Los Angeles, il concetto di *big data* ha una definizione più tecnica e una colloquiale. Nella definizione tecnica, spesso si ricorre alle tre V, ovvero Volume (possibilità di raccogliere, archiviare e processare una quantità enorme di dati, prima inimmaginabile), Velocità (la capacità di processare grandi masse di dati in tempo reale), Varietà (dati provenienti da fonti diversificate). «In termini colloquiali, *big data* coincide grossomodo con grandi quantità di dati macinate da computer potenti per scovare associazioni che altrimenti non vedremmo». Secondo la studiosa, i *big data* sono un ambiente informativo reso possibile dalla digitalizzazione di massa e associato all'uso di analitiche avanzate (come l'analisi di rete e il machine learning). In parallelo, anche 'algoritmo' ha un doppio registro: «tecnicamente è un insieme formale di istruzioni usate per analizzare dati e automatizzare decisioni» (spesso paragonato a una 'ricetta'); nell'uso corrente indica più in generale «il processo attraverso cui i computer prendono decisioni automatiche e predittive su un dataset»[17].

---

[16] G. STRATTON-A. POWELL-R. CAMERON, *Crime and justice in digital society: Towards a "digital criminology"?*, in *International Journal for Crime, Justice and Social Democracy*, 2017, vol. 6, n. 2, pp. 17-33.

[17] S. BRAYNE, *Predict and Surveil. Data, discretion and the future of policing*, cit.

Secondo boyd e Crawford, i *big data* rappresentano non solo un fenomeno tecnologico, ma anche culturale e mitologico: offrirebbero infatti la convinzione che siano in grado di fornire verità oggettive e infallibili [18]. Questa convinzione si basa sull'idea che l'analisi di grandi quantità di dati possa produrre una conoscenza 'superiore', apparentemente oggettiva e neutrale.

Anche Chan e Bennett Moses contestano l'idea secondo cui l'analisi dei dati su larga scala permetta di accedere a una conoscenza oggettiva della realtà. Questa è una mitologia, una credenza diffusa che lascia da parte il fatto che esistono dei processi di costruzione dei dati e degli algoritmi che non possono essere neutri: anche quando si presenta come puramente 'tecnica', ogni fase del trattamento dei dati (raccolta, scelta dei formati, analisi) incorpora presupposti teorici impliciti [19]. Infatti, decidere quali dati raccogliere implica una scelta basata su ciò che si considera rilevante o utile. Ad esempio, nel campo della giustizia penale, raccogliere dati sui luoghi di reato, ma non su fattori socioeconomici, presuppone una certa visione di cosa sia importante per comprendere le cause della criminalità. Allo stesso modo, le modalità con cui i dati sono definiti, categorizzati e conservati riflettono una certa ontologia – cioè un modello implicito su come il mondo è strutturato. Anche gli algoritmi di analisi, costruiti su teorie statistiche e modelli di apprendimento, sebbene spesso trattati come meri strumenti, incorporano visioni specifiche su come interpretare i dati. Ad esempio, la selezione delle variabili da includere nei modelli è guidata da ipotesi – esplicite o tacite – su cosa possa influire sul fenomeno osservato. Questo vale anche per l'interpretazione dei risultati. Infatti, anche quando l'obiettivo è solo la previsione (e non la spiegazione causale), i *pattern* individuati vengono inevitabilmente messi in relazione con teorie, anche se in modo implicito. Ogni fase è carica di scelte interpretative che richiedono riflessione teorica, anche quando questa non è esplicitamente dichiarata.

Non esiste una 'neutralità' epistemica nella costruzione o interpretazione dei dati.

Sono tre principalmente i modi in cui i dati vengono collezionati e immessi in questi immensi archivi digitali [20]: una modalità automatica, ovvero i dati vengono creati senza che noi ce ne rendiamo conto; una volontaria, in base alla quale cediamo i nostri dati in cambio di servizi (convenienza, intrattenimento, sconti, visibilità sociale); e una che coincide con la raccolta

---

[18] A. Boyd-K. Crawford, *Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon*, in *Information, Communication & Society*, 2012, vol. 15, n. 5, pp. 662-679.

[19] J. Chan-L. Bennett Moses, *Is big data challenging criminology?*, in *Theoretical Criminology*, 2016, vol. 20, n. 1, pp. 21-39.

[20] S. Milivojevic, *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century*, cit.

diretta e intenzionale da parte di autorità statali con finalità di sorveglianza, prevenzione o controllo.

Una volta collezionati, questi dati sono proprietà di sviluppatori di software, compagnie private, pubblicitari, banche, polizia, governi e tanti altri. Questi dati possono essere raccolti per essere venduti. Lo stesso flusso informativo può essere venduto anche alle forze di polizia per finalità di indagine. Il valore dei dati e l'importanza di possederli sono così alti che secondo qualcuno costituirebbero il nuovo petrolio [21] nel capitalismo della sorveglianza [22].

Per produrre conoscenza tramite i *big data* ci si avvale di processi di *data mining* [23]. Il termine *data mining* indica l'insieme di tecniche computazionali volte a estrarre, da grandi insiemi di dati, schemi ricorrenti, relazioni e modelli nascosti che non sono immediatamente evidenti. Non si tratta di una semplice descrizione statistica, ma di un processo induttivo e predittivo che utilizza algoritmi e strumenti di *machine learning* per produrre nuova conoscenza a partire dai dati grezzi. I dati digitali sono strumenti profondamente politici, in quanto incorporano e riflettono relazioni di potere che si manifestano nei processi di estrazione, gestione e utilizzo delle informazioni personali. In realtà, le scelte che gli utenti compiono – ad esempio accettare i termini di servizio o consentire l'uso dei *cookie* – avvengono all'interno di un'infrastruttura tecnologica opaca, in cui i reali margini di autonomia decisionale sono estremamente limitati [24]. Ciò che conta, in questo contesto, non è solo la raccolta dei dati, ma il modo in cui essi vengono organizzati, interpretati e messi a valore da soggetti che detengono il controllo delle infrastrutture digitali. Parlare di produzione di conoscenza attraverso i *big data* significa allora interrogare anche le logiche politiche che ne regolano l'uso e riconoscere che la costruzione della realtà algoritmica avviene spesso senza un reale coinvolgimento dei soggetti da cui quei dati provengono [25].

Lungi dall'essere una rappresentazione neutra della realtà, i dati sono socialmente costruiti [26]. Come sostiene Lupton, i dati hanno una propria vita sociale

---

[21] Clive Humby nel 2006, citato in D. WALL, *How big data feeds big crime*, in *Journal of Global History*, 2018, pp. 29-34.

[22] S. ZUBOFF, *Big other: Surveillance capitalism and the prospects of an information civilization*, in *Journal of Information Technology*, vol. 15, n. 3, pp. 75-89.

[23] D.J. HAND-H. MANNILA-P. SMYTH, *Principles of Data Mining*, Cambridge (MA), MIT Press, 2001.

[24] F. DI TANO, *Cookie, trattamento di dati personali e manipolazione del consenso*, in F. CASA (a cura di), *Intelligenza artificiale: diritto, etica e democrazia*, Bologna, il Mulino, 2025, pp. 221-236.

[25] M. SGUAZZINI, *Privacy politics: Power relations in the extraction, management, and use of personal data by non-state actors*, in *Rivista di Digital Politics*, 2022, vol. II, n. 3, pp. 399-422.

[26] S. BRAYNE, *Predict and Surveil. Data, discretion and the future of policing*, New York, New York University Press, 2021.

distinta dagli esseri umani che li hanno generati [27]. Il rischio è quindi che i processi di produzione dei dati rimangano invisibili e che dunque venga invisibilizzata l'asimmetria di potere tramite cui i dati vengono creati mentre rimane visibile solo la conoscenza che da quei dati si può trarre.

4. La polizia predittiva

Una delle applicazioni più controverse dei *big data* nel sistema della giustizia penale è quella in chiave predittiva. La polizia predittiva si propone di identificare luoghi, momenti o individui a rischio sulla base di dati storici e correlazioni statistiche, seguendo approcci che si ispirano a teorie criminologiche come la prevenzione situazionale o la vittimizzazione ripetuta [28]. La polizia predittiva si avvale di *big data* e di algoritmi per valutare con quale percentuale di possibilità una persona possa commettere un reato o in che luogo è più probabile che un reato venga commesso. Nel primo caso si parla di modelli di polizia predittiva *person-based* e l'idea di fondo è che esista un piccolo gruppo di persone responsabile della maggior parte dei crimini violenti; nel secondo caso si parla di modelli di polizia predittiva *place-based* e l'idea di fondo è il classico assunto per cui la criminalità non si distribuisce nello spazio in maniera uniforme, ma tende a concentrarsi in alcune zone.

La polizia ha da sempre fatto uso di dati e informazioni nella sua attività quotidiana: dai registri cartacei alle note di indagine, la raccolta di dati ha rappresentato un pilastro del lavoro investigativo e operativo. Tuttavia, lo sviluppo delle tecnologie digitali e dei sistemi automatizzati ha trasformato radicalmente il modo in cui le informazioni vengono acquisite, elaborate e utilizzate. Non è cambiata tanto la natura dell'attività informativa, quanto piuttosto la sua scala, profondità e sistematicità [29]. Una considerevole parte del lavoro di polizia consiste da sempre nel raccogliere informazioni, solo che tale compito è stato amplificato esponenzialmente dall'utilizzo delle tecnologie. Oggi, dunque, si collezionano dati in maniera massiva. Ma sono dati grezzi, talmente tanti che a volte superano la capacità dell'istituzione di utilizzarli e rimangono potenziale sapere di polizia, ma senza nessun sistema di *external legal accountability* [30]. L'integrazione di dati

[27] D. LUPTON, *Digital Sociology*, London, Routledge, 2015; G.J.D. SMITH-P. O'MALLEY, *Driving politics: Data-driven governance and resistance*, in *British Journal of Criminology*, 2017, vol. 57, n. 2, pp. 275-298.

[28] J. CHAN-L. BENNETT MOSES, *Is big data challenging criminology?*, cit.

[29] S. BRAYNE, *Predict and Surveil*, cit., p. 4.

[30] B. BOWLING-R. REINER-J.W.E. SHEPTYCKI, *The Politics of the Police* (5ª ed.), Oxford, Oxford University Press, 2019, p. 33.

provenienti da fonti eterogenee – giudiziarie, commerciali, sociali – ha reso possibile un livello di sorveglianza e controllo che supera di gran lunga quello delle epoche precedenti, spostando il focus dei controlli di polizia da una logica reattiva a una logica predittiva e preventiva [31]. Questa trasformazione ha determinato una vera e propria evoluzione nei modelli di polizia.

Tuttavia, i cambiamenti di polizia non si devono solo all'avanzamento tecnico ma anche al cambiamento culturale. Uno dei cambiamenti culturali più significativi è quello dell'anticipazione del rischio. La polizia da sempre può essere considerata una sorta di 'cerniera temporale': da un lato registra e gestisce ciò che è accaduto, dall'altro proietta l'azione di governo verso il futuro, cercando di prevenire i crimini prima che avvengano [32]. Tuttavia, adesso lo farebbe in chiave proattiva piuttosto che retroattiva.

Secondo Brayne, la polizia predittiva nasce dall'intersezione di due processi più ampi: l'intensificazione della sorveglianza [33] e l'ascesa dei *big data* [34]: valutazioni discrezionali di rischio vengono sostituite o integrate da punteggi numerici, i dati vengono usati con finalità predittive piuttosto che solo reattive o esplicative, e database eterogenei vengono fusi in sistemi integrati che estendono la sorveglianza ben oltre l'ambito strettamente penale. In questa prospettiva, la polizia predittiva appare non tanto come il frutto inevitabile di nuove tecnologie, quanto come l'esito di una convergenza tra dinamiche di sorveglianza e potenzialità dei *big data* [35].

---

[31] S. BRAYNE, *Predict and Surveil*, cit., p. 5.

[32] M.D. DUBBER-M. VALVERDE, *Perspectives on the power and science of police*, in M.D. DUBBER-M. VALVERDE (eds), *The New Police Science: The Police Power in Domestic and International Governance*, Stanford, Stanford University Press, 2006.

[33] L'intensificazione delle pratiche di sorveglianza in generale si riferisce alla crescita quantitativa e qualitativa dei sistemi che raccolgono e classificano informazioni sulle persone nella vita quotidiana. Questo fenomeno si manifesta in due modi complementari: da un lato, attraverso un approfondimento (*deepening*) della sorveglianza su gruppi già considerati ad alto rischio – come persone in libertà vigilata, beneficiari di assistenza pubblica o comunità marginalizzate – che vengono monitorati con strumenti sempre più sofisticati e trasversali; dall'altro, attraverso un ampliamento (*widening*) delle popolazioni sotto osservazione, con pratiche di *dragnet surveillance* che raccolgono dati in maniera indiscriminata, anche su individui che non hanno mai avuto alcun contatto diretto con le forze dell'ordine. In questo modo, la sorveglianza diventa allo stesso tempo più profonda e più estesa: segue più da vicino chi è già oggetto di attenzione, ma al tempo stesso ingloba anche chi, in passato, ne sarebbe rimasto ai margini. S. BRAYNE, *Predict and Surveil. Data, discretion and the future of policing*, cit.

[34] Questa consente nuove forme di classificazione, collegamento e previsione: dati provenienti da ambiti diversi possono essere fusi in un'unica piattaforma, analizzati algoritmicamente e trasformati in mappe di rischio, punteggi individuali di pericolosità o sistemi di allerta automatica.

[35] S. BRAYNE, *Big Data Surveillance: The Case of Policing*, in *American Sociological Review*, 2017, vol. 8, n. 1, pp. 977-1008.

Secondo Ferguson, l'emergere della polizia predittiva – che, per inciso, avviene negli Stati Uniti a cavallo degli anni Dieci del Duemila – è dovuto anche a un cambiamento culturale legato a una trasformazione nel rapporto tra polizia e comunità razzializzate nel contesto del movimento *Black lives Matter*, emerso dopo le morti di diversi cittadini afroamericani per mano della polizia [36]. *Black Lives Matter* è stata una mobilitazione nazionale – poi estesasi, seppur in misura minore, anche in altri stati del mondo – contro la violenza e l'impunità della polizia verso le comunità afroamericane. Le tecnologie predittive sono state presentate come strumenti di razionalizzazione dell'azione poliziesca, capaci di offrire una base apparentemente neutra, 'oggettiva' e priva di pregiudizi razziali per la selezione dei target e delle aree da presidiare. Tuttavia, la promessa di neutralità del *data-driven* policing appare, secondo Ferguson, più una narrazione strategica che una realtà verificabile. Infatti, i dati su cui si fondano questi sistemi sono spesso essi stessi il prodotto di pratiche storicamente discriminatorie. Negli Stati Uniti, i database di polizia riflettono e perpetuano decenni di attività mirate nelle comunità nere e latine, traducendo *bias* strutturali in metriche numeriche. Così, invece di eliminare la razzializzazione del controllo, la polizia predittiva rischia di legittimarla e istituzionalizzarla in forme più opache e meno contestabili, rafforzando una sorveglianza intensiva proprio sulle popolazioni già più colpite dalla repressione penale.

La polizia predittiva non è qualcosa di completamente nuovo, rappresenta un'evoluzione tecnologica di approcci preesistenti. Esiste una continuità strutturale tra le pratiche tradizionali di polizia e le nuove forme di *big data* policing. L'introduzione dei *big data* nella polizia non va letta come una rottura totale rispetto al passato, ma piuttosto come un intreccio di continuità e discontinuità. Da un lato, molte pratiche tradizionali di sorveglianza vengono semplicemente amplificate e quantificate: le valutazioni discrezionali di rischio fatte dagli agenti, ad esempio, sono oggi trasformate in punteggi numerici; strategie come il pattugliamento delle aree 'calde' (hotspots) sono riprese e rese più sistematiche grazie agli algoritmi; i registri cartacei sono sostituiti da database digitali, ma la logica sottostante resta simile. Dall'altro lato, l'uso dei *Big data* introduce cambiamenti sostanziali: sistemi automatici di allerta permettono di monitorare un numero di persone mai visto prima; i *database* includono anche individui senza alcun contatto diretto con la polizia; soprattutto, i dati provenienti da istituzioni diverse (scuole, sanità, servizi sociali, settore privato) vengono integrati in piattaforme uniche, ampliando enormemente l'ambito della sorveglianza. In questa prospettiva, la polizia predittiva non è né una semplice prosecuzione delle tecniche del passato, né una cesura radicale: rappresenta piuttosto un punto di

[36] G. FERGUSON, *The Rise of Big Data Policing. Surveillance, race and the future of law enforcement*, New York, New York University Press, 2017.

transizione in cui elementi già noti vengono riorganizzati e potenziati attraverso le infrastrutture digitali dei *big data* [37].

5. I rischi della polizia predittiva

Le ricerche critiche sulla polizia predittiva concordano nel mostrare come i sistemi di analisi predittiva non siano strumenti neutrali, ma si fondino su basi di dati prodotte nel tempo da pratiche di polizia condizionate da logiche razziali, socioeconomiche e spaziali. Gli algoritmi, lungi dal correggere tali distorsioni, tendono a riproporle sotto forme più difficili da individuare e contestare, conferendo un'aura di scientificità a ciò che, in sostanza, rappresenta la traduzione automatizzata di pregiudizi strutturali.

Questa legittimazione algoritmica delle decisioni di polizia risulta particolarmente insidiosa. I numeri cessano di essere semplici strumenti descrittivi per assumere la funzione di veri e propri dispositivi di autorità, in grado di restringere lo spazio del dibattito democratico e giuridico. A ciò si sommano l'impiego di un linguaggio tecnico e l'opacità dei modelli computazionali – le cosiddette *black boxes* – che rendono arduo, se non impossibile, comprendere i processi decisionali sottesi. Tale opacità finisce per schermare l'operato delle forze dell'ordine dalla critica pubblica e dal controllo istituzionale. In pratica, la dipendenza dagli esiti algoritmici tende a erodere l'autonomia decisionale degli operatori: il calcolo sostituisce progressivamente la scelta discrezionale. L'agente può legittimare le proprie scelte appellandosi alla 'voce' dell'algoritmo, giustificando le proprie decisioni attraverso il riferimento all'output del sistema, con un conseguente spostamento della responsabilità dall'individuo alla tecnologia, percepita come neutrale e scientificamente fondata.

Pur in presenza di valutazioni divergenti tra gli stessi agenti sull'efficacia e sull'opportunità di impiegare strumenti predittivi [38], è ormai evidente che la polizia predittiva non si limita a ridefinire le strategie operative: essa trasforma in profondità le relazioni di potere, i meccanismi di *accountability* e le forme di *agency* che strutturano il sistema di sicurezza. Comprendere chi eserciti effettivamente il potere decisionale e come questo si traduca in azione è indispensabile per attribuire responsabilità e valutare le ricadute delle decisioni assunte. Non si tratta di una questione meramente teorica: il rischio è che scelte

[37] S. BRAYNE, *Predict and Surveil. Data, discretion and the future of policing*, cit.

[38] L. NEIVA-R. GRANJA-H. MACHADO, *Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union*, in *Policing and Society*, 2022, vol. 32, n. 10, pp. 1167-1179; L. NEIVA-H. MACHADO-S. SILVA, *The views about big data among professionals of police forces: A scoping review of empirical studies*, in *International Journal of Police Science and Management*, 2023, vol. 25, n. 2, pp. 208-220.

intrinsecamente politiche – come la determinazione di ciò che costituisce un 'rischio' per l'ordine pubblico – vengano presentate come valutazioni tecniche, sottraendole così al controllo democratico e normativo.

5.1. Razzializzazione

Lungi dal costituire uno strumento utile a limitare la profilazione razziale, i *big data* riproducono le asimmetrie di potere delle società in cui si formano. Uno dei problemi dell'utilizzo delle tecnologie *data-driven* risiede nella qualità dei dati utilizzati per predire il comportamento criminale: se i dati sono già falsati dai processi di razzializzazione, la tecnologia *data-driven* non potrà che riprodurre tali processi di razzializzazione.

PredPol è uno dei sistemi di *predictive policing* più noti e controversi. Sviluppato da ricercatori dell'UCLA e commercializzato dal 2012, si tratta di uno strumento *place-based*, che elabora dati storici sulla criminalità per produrre *predicted boxes,* piccole aree quadrate (circa 150 metri per lato) in cui è più probabile che, nelle successive 12 ore, avvenga un reato. Gli agenti ricevono queste mappe all'inizio del turno e vengono incoraggiati a trascorrere più tempo in queste aree. Il funzionamento di *PredPol* si basa su un algoritmo proprietario che utilizza tre *input* principali: il tipo di reato, il luogo e il momento in cui esso si è verificato. Il modello è costruito sulla teoria del *near-repeat*, secondo cui, dopo che un crimine si è verificato in un'area, le zone circostanti presentano un rischio aumentato di reati simili. L'algoritmo si alimenta di dieci anni di dati, attribuendo maggior peso a quelli più recenti, e genera così le mappe di rischio. Questo approccio ha mostrato risultati discreti per reati legati alla proprietà (ad esempio furti), mentre si è dimostrato molto meno efficace nel prevenire reati violenti. Il problema più rilevante, tuttavia, riguarda i suoi effetti sociali. Se i dati su cui *PredPol* si addestra riflettono *pattern* storici di sorveglianza e di arresti sproporzionati nelle comunità minoritarie, l'algoritmo finisce per riprodurre e amplificare queste stesse disuguaglianze. Come visto negli Stati Uniti, le aree a prevalenza afroamericana o latino-americana, già fortemente pattugliate, risultano più frequentemente contrassegnate come 'zone a rischio', generando un *feedback loop*: maggiore presenza della polizia produce più controlli, più segnalazioni e quindi più dati 'negativi' che confermano falsamente la pericolosità di quei quartieri. In questo modo, una tecnologia presentata come 'scientifica' e 'oggettiva' rischia di mascherare pratiche di profilazione razziale già esistenti, rendendole meno visibili ma più radicate. *PredPol* diventa quindi un esempio emblematico di come il *predictive policing* possa tradursi non in un superamento dei *bias* umani, bensì nella loro istituzionalizzazione attraverso strumenti algoritmici [39].

[39] S. BRAYNE, *Predict and Surveil. Data, discretion and the future of policing*, cit.

5.2. *Privacy*

I rischi per la privacy legati alla polizia predittiva derivano principalmente dalla perdita di anonimato nello spazio pubblico e dalla costante raccolta di dati comportamentali, anche su cittadini che non sono sospettati di alcun reato. Questo significa che dati personali su individui innocenti vengono raccolti, analizzati e utilizzati per anticipare comportamenti futuri, spesso senza che questi soggetti ne siano consapevoli o abbiano fornito alcun consenso. Il monitoraggio tramite telecamere intelligenti può registrare ogni movimento o interazione urbana, anche in assenza di un sospetto specifico. Con notevoli differenze rispetto a ciò che è lecito e ciò che non lo è a seconda delle giurisdizioni, le forze dell'ordine possono utilizzare dati personali raccolti da fonti come social media, registri commerciali, scuole e sistemi sanitari, creando una visione completa ma invasiva della vita privata di un individuo. Inoltre, spesso le persone monitorate non sanno di essere profilate, non possono accedere ai dati raccolti su di loro e non hanno modo di contestare l'inclusione in una zona ad alto rischio o in una 'lista di sorvegliati' [40].

Il riconoscimento facciale in tempo reale (*Live Facial Recognition*, LFR) rappresenta una delle forme più invasive di sorveglianza contemporanea, con implicazioni profonde per la *privacy* e per i diritti fondamentali. Come sottolineano Papada e Vradis, l'uso diffuso di queste tecnologie nello spazio urbano produce un regime di sorveglianza di massa, in cui la semplice presenza nello spazio pubblico può trasformarsi in un atto sospetto, potenzialmente oggetto di schedatura e analisi biometrica [41]. Il volto, parte intima e identitaria del corpo, diventa un dato costantemente catturato, archiviato e confrontato con database di polizia, riducendo l'anonimato urbano e trasformando la città da luogo di libertà a spazio di sospetto permanente. È emblematico il caso della *South Wales Police a Cardiff*, che aveva introdotto sistemi di LFR per monitorare eventi pubblici e strade cittadine, confrontando i volti dei passanti con liste di persone di interesse. Nel 2020 la *Court of Appeal* per Inghilterra e Galles ha dichiarato tale pratica illegale, ritenendo che violasse il diritto alla *privacy* sancito dalla Convenzione europea dei diritti dell'uomo, le normative sulla protezione dei dati e i principi di uguaglianza. La sentenza ha messo in luce gravi carenze: criteri opachi per l'inclusione nelle *watchlists*, assenza di linee guida chiare per limitare la discrezionalità della polizia, mancata valutazione d'impatto sui diritti

---

[40] G. FERGUSON, *The Rise of Big data Policing*, cit., pp. 97-106.

[41] E. PAPADA-A. VRADIS, *The birth of spatial transgression: genealogies and regulatory instruments in the use of facial recognition technologies in the UK*, in V. GALIS-H.O.I. GUNDHUS-A. VRADIS (eds), *Critical Perspectives on Predictive Policing: Anticipating Proof?*, Cheltenham-Northampton, Edward Elgar Publishing, 2025, pp. 43-64.

fondamentali. Tuttavia, questa decisione non ha comportato l'abbandono definitivo delle tecnologie di riconoscimento facciale. Al contrario, esse tendono a riemergere in forme ridefinite e circoscritte, ad esempio per il monitoraggio di grandi eventi sportivi, concerti o aree commerciali, spesso giustificate da esigenze di sicurezza. Tale persistenza dimostra come, anche di fronte a limiti giuridici espliciti, la pressione istituzionale e tecnologica favorisca la continuità della sorveglianza biometrica, aggravando i rischi di erosione della *privacy*, discriminazione algoritmica e compressione delle libertà civili nello spazio urbano [42].

5.3. Ridefinizione della cittadinanza

Un aspetto centrale del controllo *data-driven* riguarda le conseguenze sociali dell'uso dei *big data* da parte della polizia. In linea teorica, la digitalizzazione potrebbe avere un effetto positivo, perché riduce la dipendenza esclusiva del meccanismo decisionale dal giudizio discrezionale degli agenti. Inoltre, i dati digitali consentono di monitorare le attività di polizia. Tuttavia, nella pratica i *big data* tendono spesso a rafforzare e riprodurre disuguaglianze sociali preesistenti. Primo, la sorveglianza diventa più profonda per chi è già nel raggio d'azione della giustizia penale: le persone con precedenti, o già classificate come 'a rischio', vengono seguite attraverso una molteplicità di banche dati che si intrecciano, moltiplicando le occasioni di controllo. Secondo, la sorveglianza si amplia verso nuovi soggetti: i sistemi digitali includono dati di individui che non hanno mai avuto un contatto diretto con la polizia, creando un'enorme 'rete a strascico' che ingloba fasce sempre più ampie di cittadini. Terzo, questa nuova configurazione può produrre effetti collaterali paradossali: negli Stati Uniti, per timore che le informazioni personali possano finire nei *database* della polizia, alcuni cittadini evitano scuole, ospedali o servizi sociali, cioè proprio quelle istituzioni fondamentali per l'integrazione e il benessere collettivo [43].

I *big data* contribuiscono così a ridefinire i confini della cittadinanza e a rafforzare forme di disuguaglianza sociale, incidendo in profondità sul rapporto tra individui, istituzioni e giustizia penale. Ovvero, la polizia predittiva, trasformando le modalità attraverso cui vengono esercitati il controllo e la sorveglianza, ridefinisce anche chi è considerato un 'buon cittadino' o un soggetto 'a rischio' [44]. I sistemi predittivi non operano nel vuoto. Si basano su dati preesistenti, raccolti in modo storicamente selettivo e spesso distorto. Questo

[42] *Ibid*.

[43] S. BRAYNE, *Big Data Surveillance: The Case of Policing*, cit.

[44] V. GALIS-H. OPPEN GUNDHUS-A. VRADIS, *Critical Perspectives on Predictive Policing: Anticipating Proof?*, cit.

significa che alcuni gruppi sociali – soprattutto minoranze razzializzate o persone che vivono in aree già fortemente sorvegliate – vengono più facilmente etichettate come 'a rischio', anche in assenza di comportamenti illeciti. La loro cittadinanza, pur formalmente piena, viene materialmente erosa, perché soggetta a una sorveglianza continua e a un trattamento differenziato. Con la polizia predittiva, non è più necessario 'fare qualcosa' per attirare l'attenzione della polizia: può bastare accompagnarsi a un 'profilo' sbagliato, trovarsi in una rete sociale sorvegliata, o abitare in un quartiere classificato come problematico. Questo sposta il baricentro della cittadinanza da un'idea di diritti universali a una logica di rischio calcolato, dove alcune biografie valgono meno di altre agli occhi del sistema. Questo mina i principi fondamentali della cittadinanza democratica, basata sulla presunzione di innocenza e sull'uguaglianza di trattamento, e trasforma la relazione tra individuo e Stato da un rapporto fondato sui diritti a uno fondato sulla gestione del rischio [45].

5.4. La performatività dei *big data*

Una delle questioni più complesse che emergono negli studi critici sui *big data* è la consapevolezza che i dati non descrivono la realtà in maniera neutra, ma «agiscono su ciò che descrivono e retroagiscono su chi li utilizza e li costruisce»[46]. La quantificazione ha effetti performativi e trasformativi della realtà. Dire che i dati sono performativi significa affermare che essi siano in grado di costituire la realtà, di plasmarla. I dati retroagiscono su chi li produce e la realtà viene ricostruita anche in base ai rapporti di potere comunque presenti nei processi di costruzione dei dati. Parlare della produzione di conoscenza in relazione alla tecnologia *data-driven* equivale a parlare delle strutture di potere insite nei processi di costruzione di *dataset* e *software*, dell'accesso ai dati e della diversa possibilità che diversi soggetti hanno di comprendere come i dati vengono trasformati in informazioni.

Kaufmann e Leese, analizzando il funzionamento di software algoritmici utilizzati nella sicurezza pubblica in Germania e Svizzera, introducono il concetto di *information in-formation* per descrivere la natura instabile, situata e trasformativa dei dati [47]. Con questa espressione, gli autori intendono sottolineare che

---

[45] *Ibidem.*

[46] B. Aragona, S. Stefanizzi, *Società digitale: interrogativi, aree di ricerca e ruolo della sociologia*, in *Sociologia Italiana*, 2024, 7, pp. 7-19.

[47] M. Kaufmann-M. Leese, *Information In-Formation: Algorithmic Policing and the Life of Data*, in V. Badalič-A. Završnik (a cura di), *Automating Crime Prevention, Surveillance, and Military Operations*, Cham, Springer, 2021, pp. 69-83.

i dati non sono entità fisse, già date e neutrali, ma sono continuamente in formazione, ossia soggette a processi di selezione, interpretazione, modifica e riutilizzo, sia da parte di attori umani (come poliziotti, analisti, operatori) sia da parte di sistemi automatici e infrastrutture digitali. I dati sono, in altre parole, 'vivi' (*lively*), nel senso che mutano costantemente lungo tutto il loro ciclo di vita: dalla raccolta alla classificazione, dalla pulizia all'analisi, fino al loro riutilizzo in nuovi contesti. Questo carattere dinamico si manifesta, ad esempio, nel momento della registrazione iniziale di un evento criminale. La distinzione tra reati come furto, rapina o danneggiamento non è puramente oggettiva, ma dipende da come l'agente interpreta la scena, compila il modulo digitale e seleziona le categorie predefinite. Queste decisioni, spesso prese in condizioni di urgenza o sotto vincoli operativi, generano dati parziali e potenzialmente distorti. Tuttavia, tali dati alimentano i modelli di previsione, che a loro volta guidano le decisioni operative della polizia – ad esempio su dove concentrare le pattuglie. Questo genera un effetto circolare: le zone già sottoposte a sorveglianza producono più dati, che giustificano ulteriori interventi, in un ciclo autoreferenziale che tende a rafforzare disuguaglianze preesistenti. La nozione di *information in-formation* aiuta dunque a comprendere come la performatività dei dati derivi non solo dai risultati finali prodotti dagli algoritmi, ma anche dai processi, spesso invisibili, attraverso cui i dati stessi prendono forma. In questa prospettiva, i dati non sono soltanto strumenti di conoscenza, ma anche dispositivi di potere che, attraverso pratiche quotidiane e tecnologie computazionali, contribuiscono attivamente alla costruzione della realtà sociale che pretendono di rappresentare.

Come osserva Ferguson, ciò che rende i *Big data* davvero operativi non è soltanto la quantità o la varietà delle informazioni raccolte, ma l'insieme di tecnologie, algoritmi e potenza computazionale che permettono di renderli leggibili, comparabili e utilizzabili. «*What Big data knows is one thing, but the technology used to manipulate and organize that data is the bigger thing*» [48]. Tuttavia, come sottolineano Kaufmann e Leese, questi strumenti operano su dati che non sono entità stabili e neutrali, ma prodotti dinamici di pratiche sociali, istituzionali e tecniche. La performatività dei dati, quindi, emerge dall'interazione tra la loro formazione situata e le infrastrutture computazionali che li classificano, li interpretano e li mobilitano. In questo senso, la costruzione della realtà algoritmica non è riconducibile né ai soli dati né ai soli algoritmi, ma va intesa come il risultato di un intreccio tra potere epistemico, pratiche operative e tecnologia. Come suggerisce la prospettiva decoloniale, sia i dati sia gli algoritmi si inscrivono in infrastrutture che riflettono gerarchie globali, interessi economici e rapporti di potere storicamente radicati. La produzione di conoscenza

[48] G. FERGUSON, *The rise of big data policing*, cit., p. 18.

algoritmica non è dunque soltanto un processo tecnico, ma anche un progetto politico che contribuisce a definire chi può conoscere, cosa può essere conosciuto e in quali termini [49].

5.5. L'ingerenza del settore privato

Esiste un settore privato in espansione che si occupa di collezionare e vendere i dati personali dei cittadini. Molte agenzie integrano i propri database interni con informazioni commerciali, come registri dei social media, dati sul traffico o comportamenti dei consumatori, acquistati da imprese private. Questa pratica consente analisi più ampie, ma solleva preoccupazioni sull'accuratezza dei dati, sul loro uso etico e, non da ultimo, sulle implicazioni per la *privacy* derivanti dall'integrazione di tali dati. Le ricerche condotte negli Stati Uniti sulla polizia predittiva hanno mostrato che le aziende private forniscono anche dati direttamente alle forze dell'ordine [50], con il risultato che possono arrivare all'attenzione delle forze dell'ordine anche i dati di persone che di solito non facevano esperienza di controlli di polizia. Anche dati che non sono direttamente interessanti per scopi di *law enforcement* o condotte non penalmente rilevanti possono entrare nella sfera d'azione della polizia.

Questo però non accade solo negli Stati Uniti. I dati PNR (*Passenger Name Record*) – inizialmente raccolti dalle compagnie aeree per scopi commerciali – sono diventati una pietra angolare delle operazioni di sicurezza pubblica [51]. Le compagnie aeree, in quanto entità private, raccolgono e trasmettono i dati PNR alle *Passenger Information Units* (PIU) gestite dai governi, in base a quadri normativi come la Direttiva PNR dell'Unione Europea. Questi database contengono informazioni sensibili sui passeggeri, come identità, itinerari di viaggio, metodi di pagamento e preferenze. Sebbene la raccolta sia pensata per la gestione dei clienti, il loro riutilizzo a fini di sicurezza statale rivela la privatizzazione di fonti di dati essenziali. Agendo come intermediari, le compagnie aeree trasformano dati commerciali in *intelligence* operativa, incorporando processi privati nell'ecosistema più ampio della sorveglianza. La dipendenza da attori privati va oltre la raccolta dati, includendo anche le infrastrutture tecnologiche che permettono l'elaborazione e l'analisi dei *Big data*. Le PIU si affidano a strumenti di integrazione e software, spesso sviluppati o gestiti in collaborazione con fornitori privati, per analizzare e incrociare i dati PNR con altri

---

[49] M. KAUFMANN-M. LEESE, *Information In-Formation: Algorithmic Policing and the Life of Data*, cit.

[50] S. BRAYNE, *Predict and Surveil. Data, discretion and the future of policing*, cit.

[51] G. GLOUFTSIOS-M. LEESE, *Epistemic fusion: Passenger Information Units and the making of international security*, in *Review of International Studies*, 2023, vol. 49, n. 1, pp. 125-142.

database di sicurezza pubblica, come le liste di sorveglianza o i sistemi di immigrazione. Questi strumenti permettono ai governi di operare su *dataset* enormi, ma al contempo inseriscono interessi privati nei quadri di sicurezza pubblica. Inoltre, le imprecisioni intrinseche dei dati PNR autocompilati – come errori di battitura o informazioni incomplete – richiedono ulteriori misure di controllo della qualità. Le compagnie aeree, in quanto fornitori di dati, influenzano significativamente la qualità e l'affidabilità delle informazioni trasmesse alle PIU, modellando indirettamente l'efficacia delle analisi di sicurezza [52].

Il settore privato svolge un ruolo fondamentale anche nel plasmare il modo in cui le forze dell'ordine utilizzano i *big data* per il controllo, la prevenzione e l'indagine sui reati. I dipartimenti di polizia si affidano sempre più frequentemente (ancora poco in Italia, fortunatamente) a *software* di polizia predittiva sviluppati da aziende private, integrando nei loro sistemi algoritmi proprietari.

Proprio il fatto che alcuni algoritmi sono di proprietà di compagnie private alimenta l'opacità di questi strumenti, e rende difficile sia per la polizia comprendere come la macchina sia arrivata alla decisione, sia per il pubblico stabilire di chi sia la responsabilità delle decisioni che infine la polizia prende. Per ovviare a questo problema, alcuni dipartimenti di polizia hanno scelto di sviluppare software alternativi interni (in Italia è il caso del software *Xlaw* nella questura di Napoli), con l'obiettivo di ridurre la dipendenza dai privati e garantire una maggiore comprensione dei processi algoritmici [53].

Il rapporto tra le forze dell'ordine pubbliche e le imprese tecnologiche private influenza non solo lo sviluppo degli strumenti di analisi criminale, ma anche il modo in cui le teorie criminologiche vengono applicate. Molti algoritmi si fondano su definizioni ristrette di criminalità, escludendo fattori strutturali come povertà o disuguaglianza, che invece molte teorie criminologiche – forse quelle più critiche – considerano fondamentali per comprendere i fenomeni criminali [54]. Concetti come l'*hotspot policing* o i punteggi di valutazione del rischio dominano i *framework* algoritmici, mentre teorie sociali più ampie che affrontano le disuguaglianze sistemiche o le cause profonde della criminalità vengono marginalizzate. Questa dinamica riflette la tensione tra le radici accademiche della criminologia e la sua traduzione operativa in strumenti algoritmici progettati per mercati guidati dal profitto.

---

[52] G. Glouftsios-M. Leese, *Epistemic fusion: Passenger Information Units and the making of international security*, cit.

[53] L. Neiva-H. Machado-S. Silva, *The views about big data among professionals of police forces: A scoping review of empirical studies*, cit.

[54] M. Kaufmann-S. Egbert-M. Leese, *Predictive policing and the politics of patterns*, in *British Journal of Criminology*, 2019, vol. 59, n. 3, pp. 674-692.

Questo certamente si deve anche a un cambiamento del sapere criminologico, che per adeguarsi alle nuove richieste, ha rinnovato le proprie spiegazioni teoriche, dando sempre più spazio, ad esempio, alle metodologie quantitative piuttosto che alle qualitative. Come spiegano efficacemente Karlsoom e Galis, queste trasformazioni della criminologia hanno rappresentato il motore per la costruzione di modelli quantitativi che, in epoca contemporanea, sono stati progressivamente digitalizzati e automatizzati [55]. La diffusione delle teorie di prevenzione situazionale negli anni Novanta ha favorito lo sviluppo dell'analisi dei *crime hot spots* e, successivamente, la creazione nel Regno Unito di una delle prime applicazioni di polizia predittiva, nota come *ProMap* [56].

Se le collaborazioni con il settore privato potenziano le capacità analitiche della polizia, comportano anche il rischio di non solo perpetuare *bias* e restringere l'orizzonte dell'indagine criminologica, ma anche di privilegiare gli interessi commerciali rispetto alla responsabilità pubblica. Infatti, i *software* proprietari tendono a privilegiare logiche di profitto e di mercato rispetto alla trasparenza e alle considerazioni etiche legate al loro uso.

Le aziende private giocano anche un ruolo significativo nel determinare come questi strumenti vengano adottati e utilizzati. Imprese come Palantir promuovono attivamente i propri prodotti attraverso conferenze per le forze dell'ordine, presentando casi d'uso che sfumano i confini tra applicazioni militari e sicurezza pubblica [57]. Gli interessi del settore privato influenzano così lo sviluppo degli algoritmi di analisi criminale, privilegiando sistemi proprietari rispetto a soluzioni trasparenti e collaborative [58]. Con l'evoluzione delle tecnologie di polizia predittiva, la dipendenza dai fornitori privati rischia di consolidare pregiudizi non controllati nelle pratiche delle forze dell'ordine, sottolineando la necessità di una maggiore supervisione anche da parte di organismi esterni e dell'opinione pubblica e di un'analisi critica di tali partnership [59]. Questa mancanza di trasparenza rende difficile per le forze dell'ordine – o per il pubblico – valutare il funzionamento di tali algoritmi o mettere in discussione le assunzioni su cui si fondano.

---

[55] B. KARLSSON-V. GALIS, *POL-INTEL: Predictive policing and the politics of data integration in Denmark*, cit., p. 123 ss.; S. EGBERT-M. LEESE, *Criminal Futures: Predictive Policing and Everyday Police Work*, London-New York, Routledge, 2021.

[56] R.V. BRAKEL, *Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing*, in B. VAN DER SLOOT-D. BROEDERS-E. SCHRIJVERS (eds), *Exploring the Boundaries of Big Data*, Amsterdam, Amsterdam University Press, 2016.

[57] S. BRAYNE, *Predict and Surveil*, cit.

[58] K. HANNAH-MOFFAT, *Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates*, in *Theoretical Criminology*, 2018, vol. 23, n. 4, pp. 453-470.

[59] M. KAUFMANN-S. EGBERT-M. LEESE, *Predictive policing and the politics of patterns*, in *British Journal of Criminology*, 2019, vol. 59, n. 3, pp. 674-692.

6. Conclusioni

Non esistono dati 'neutri', ma scelte su cosa raccogliere, come etichettare e come interpretare. Tali scelte riflettono valori e priorità [60]. D'altronde, «i modelli siano opinioni incorporate nella matematica» [61]. Ovvero, i *software* di analisi non sono strumenti neutri, bensì veicolano le concezioni di chi li ha creati. Inoltre, l'affidabilità dei sistemi predittivi dipende anche dalla qualità dei dati di partenza. Nel settore della giustizia penale, tuttavia, i dati risultano spesso parziali o distorti [62]. Questo squilibrio alimenta il cosiddetto *base-rate problem*: la polizia raccoglie enormi quantità di dati, ma di qualità molto variabile e parziali. Tali database, già intrisi di *bias*, finiscono per trasferire questi stessi bias nei modelli predittivi. Si conferma così il principio del *garbage in, garbage out*: dati di scarsa qualità (*garbage in*) generano modelli fallaci (*garbage out*). Završnik, come altri autori, insiste sul carattere politico della produzione dei dati: qualcuno deve sempre decidere cosa rendere visibile, cosa proteggere e cosa interpretare [63].

La costruzione di database e algoritmi in giustizia penale è tutt'altro che un processo tecnico e neutrale, ma rappresenta una pratica carica di scelte politiche e sociali, capace di consolidare rapporti di potere e di riprodurre disuguaglianze sistemiche sotto l'apparenza di neutralità scientifica.

Gli studi criminologici e critici sui sistemi del controllo *data-driven* nelle forze di polizia in Europa condividono la tesi per cui le tecnologie di polizia predittiva non siano strumenti neutri, ma dispositivi sociotecnici che incarnano specifiche visioni politiche e culturali della sicurezza [64]. Tali ricerche condividono un quadro teorico per cui la polizia predittiva non rappresenti soltanto una questione tecnica di efficienza, ma soprattutto un fenomeno politico e culturale che ridefinisce il rapporto tra polizia, cittadini e tecnologia. Questi software mostrano quanto le promesse di una polizia basata sui dati si intreccino con logiche di potere, strategie di governance e narrazioni pubbliche che cercano di legittimare l'uso di strumenti complessi e opachi [65]. L'uso dell'intelligenza

---

[60] A. ZAVRŠNIK, *Algorithmic justice: Algorithms and big data in criminal justice settings*, in *European Journal of Criminology*, 2019, vol. 18, n. 5, pp. 632-642.

[61] C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Crown Random House, 2016.

[62] A. ZAVRŠNIK, *Big Data*, in M. KAUFMANN-H.M. LOMELL (a cura di), *De Gruyter Handbook of Digital Criminology*, Berlin-Boston, De Gruyter, 2025, pp. 107-114., p. 111.

[63] L. GITELMAN (a cura di), *Raw Data Is an Oxymoron*, Cambridge (MA), MIT Press, 2013.

[64] V. GALIS-H.O.I. GUNDHUS-A. VRADIS (eds), *Critical Perspectives on Predictive Policing: Anticipating Proof*?, cit.

[65] B. KARLSSON-V. GALIS, *POL-INTEL: Predictive policing and the politics of data integration in Denmark*, cit.

artificiale nelle pratiche di polizia richiede un costante scrutinio critico poiché i *pattern* prodotti da questi sistemi, e che guidano operativamente le forze dell'ordine, tendono a mascherare le assunzioni, i valori e le strutture decisionali sottostanti, che rimangono spesso invisibili e non verificabili [66].

La predizione algoritmica nel contesto della polizia predittiva non è mai solo un fatto tecnico, ma si fonda su 'pratiche sociomateriali' (*sociomaterial practices*), espressione con cui si fa riferimento all'intreccio di pratiche sociali (decisioni politiche, priorità istituzionali, visioni culturali della sicurezza) e materiali (dati raccolti, infrastrutture tecnologiche, modelli statistici) che insieme danno forma ai processi predittivi. In altre parole, gli algoritmi non "parlano da soli": il modo in cui sono costruiti e impiegati riflette scelte sociali, valori e contesti specifici. La 'materialità' delle pratiche si vede nel codice, nei database e nei sistemi tecnici; la dimensione 'sociale' si manifesta nelle decisioni su come questi strumenti vengono applicati, interpretati e giustificati. Meijer e Wessels collegano questa idea al fatto che le correlazioni trovate dagli algoritmi rischiano di essere prese come verità oggettive, ma in realtà derivano da un contesto socio-materiale che condiziona sia ciò che viene predetto sia il modo in cui le previsioni vengono usate. In questo senso, non possiamo separare la tecnica (gli algoritmi) dalla società che li produce e li utilizza [67]. Ad esempio, includere o escludere certi reati dai *database* non è un'operazione neutra, ma influenza direttamente le previsioni; l'algoritmo produce mappe di *hotspots*, ma è la polizia a decidere come e quanto pattugliare quelle aree. La predizione tecnica, dunque, si intreccia con le pratiche sociali della polizia e con le percezioni pubbliche di sicurezza; anche quando un algoritmo segnala un rischio elevato, il modo in cui le autorità interpretano quella previsione dipende da norme giuridiche, priorità istituzionali o pressioni politiche. In altre parole, la predizione non nasce solo dal calcolo algoritmico, ma da un'ibridazione costante tra tecnologia e società: *database*, *software* e modelli matematici sono materiali, ma sono plasmati da pratiche sociali che ne orientano la forma e l'uso.

La predizione emerge come il prodotto di processi diversi (raccolta dati, costruzione degli algoritmi, implementazione operativa, effetti sociali), tanto che molte criticità emergono non tanto dall'algoritmo in sé, quanto dal modo in cui i risultati vengono interpretati e utilizzati. Se esiste un problema di discriminazione e di selettività del controllo, questa va ricercata non tanto – o non unicamente – nell'utilizzo delle tecnologie *data-driven* ma è un problema antico

---

[66] M. KAUFMANN, *AI in policing and law enforcement*, in *Handbook on Public Policy and Artificial Intelligence*, Cheltenham-Northampton, Edward Elgar Publishing, 2024, pp. 295-304.

[67] A. MEIJER-M. WESSELS, *Predictive Policing: Review of Benefits and Drawbacks*, in *International Journal of Public Administration*, 2019, vol. 42, n. 12, pp. 1031-1039.

come la polizia, e ha a che fare con la sua cultura, il suo potere discrezionale e il suo mandato [68]: mantenere l'ordine e, al contempo, prendere delle decisioni su cosa sia ordine e cosa no [69].

Un discorso va fatto anche sulla legittimità della polizia algoritmica. Come sostengono Mejer e Wessels, non è sufficiente che un sistema predittivo sia tecnicamente accurato: la sua accettabilità sociale e politica dipende dalla possibilità per i cittadini e gli elettori di comprendere, valutare e controllare le scelte incorporate negli algoritmi. Ciò implica la necessità di maggiore trasparenza procedurale, *audit* indipendenti e strumenti di contestazione pubblica, che mancano ancora, ma senza i quali la fiducia nella polizia rischia di deteriorarsi [70].

Tuttavia, la richiesta di trasparenza rischia di essere insufficiente. Infatti, tecniche come il *machine learning* e le reti neurali rimangono per loro natura delle *black boxes*, ed è illusoria la richiesta di rendere questi processi algoritmici completamente spiegabili. Završnik mette in guardia contro la tentazione di ridurre questioni complesse a semplici calcoli. Il nodo non si esaurisce nella richiesta di algoritmi 'più trasparenti': la vera domanda è se tali strumenti contribuiscano davvero a migliorare la società. Si pensi, ad esempio, agli algoritmi che stimano il rischio di recidiva o la probabilità che un imputato si presenti al processo. Invece di concentrarsi esclusivamente su chi non si presenterà, sarebbe forse più utile indagare le cause sociali di tale comportamento: si tratta di difficoltà economiche che impediscono di comparire in giudizio? Della mancanza di mezzi di trasporto? Porre questo tipo di domande significa adottare un approccio radicalmente diverso da quello che le risposte tecniche, da sole, sono in grado di offrire [71]. Certo, adottare un approccio di questo tipo significa anche muoversi in un campo interdisciplinare nell'analisi della situazione, nell'individuazione dei problemi e nell'elaborazione delle soluzioni. Lo studio della *sicurezza dai dati* nelle tecnologie di controllo *data-driven* in uso alle forze di polizia richiede di condurre ricerca empirica a cavallo della sociologia, dell'informatica giuridica e delle scienze computazionali, per comprendere da un lato il funzionamento tecnico dei dispositivi e dall'altro le ripercussioni *reali* sul sociale, nonché il ruolo del sociale nella costruzione dei dispositivi. La ricerca empirica va poi inserita in uno studio complesso e puntuale del quadro normativo di riferimento che pone limiti all'utilizzo degli strumenti, anche in sede processuale. In collaborazione con le altre discipline, la criminologia può offrire riflessioni ponderate sul tipo di teorie e assunti criminologici che informano le tecnologie *data-driven* e sulle loro conseguenze applicative. Può inoltre

---

[68] *Ibid.*

[69] G. FABINI-E. GARGIULO-D. TUZZA, *Polizia: un vocabolario dell'ordine*, cit.

[70] A. MEIJER-M. WESSELS, *Predictive Policing: Review of Benefits and Drawbacks*, cit.

[71] A. ZAVRŠNIK, *Algorithmic justice: Algorithms and big data in criminal justice settings*, cit.

suggerire possibili miglioramenti (sia nella costruzione dei *software* sia nell'uso che ne viene fatto) alla luce della riflessione propria della criminologia critica rispetto alle tematiche della sicurezza, del controllo e della criminalità. Tale riflessione risulta utile alla comprensione tanto dei meccanismi 'tradizionali' di controllo e di costruzione della criminalità quanto del loro corrispettivo nelle società digitali.

La posta in gioco, in questo cambio di paradigma, è allo stesso tempo teorica e politica: non si tratta solo di comprendere come cambia il crimine con il digitale, ma di interrogarsi su chi viene reso visibile o invisibile, su quali soggettività vengono profilate, criminalizzate, neutralizzate o escluse, e su quali forme di giustizia siano ancora possibili in un mondo governato da algoritmi, piattaforme e infrastrutture opache.

Capitolo 12

Il *Cyber Resilience Act* come strumento per la protezione dei valori dell'UE? Tra esigenze di sicurezza dei prodotti e tutela dei diritti fondamentali dei singoli

Virginia Remondino [*]

Abstract: Il Regolamento 2024/2847 sulla ciberresilienza ("*Cyber Resilience Act*" o "CRA"), adottato dal Parlamento europeo e dal Consiglio nell'ottobre del 2024, rappresenta un nuovo strumento all'interno del "*toolkit*" dell'Unione europea in materia di *cybersecurity*, introducendo specifici requisiti essenziali di cybersicurezza per i prodotti con elementi digitali messi a disposizione sul mercato interno. Ciò, asseritamente, non solo al fine di rafforzare la sicurezza complessiva, ma anche per proteggere i diritti e le libertà fondamentali riconosciuti in capo ai singoli. Il presente contributo intende quindi esaminare l'apporto offerto dal CRA alla tutela dei diritti in parola, come suggerito dalla Commissione europea nella relativa Proposta di regolamento. L'indagine prende le mosse dalla ricostruzione del paradigma "securitario-valoriale" posto alla base dell'approccio dell'Unione in materia di prodotti connessi, come risulta dall'analisi dei documenti di *policy* adottati delle Istituzioni dell'UE. Successivamente, ci si sofferma sui profili di tutela dei diritti fondamentali ai sensi del *Cyber Resilience Act*. In particolare, si evidenzia che tali diritti non rivestono un ruolo di primo piano con riguardo tanto all'impianto sistemico del CRA, quanto alla definizione dei requisiti essenziali di cybersicurezza dei prodotti con elementi digitali. Detti diritti, tuttavia, assumono rilievo in relazione alle procedure di vigilanza del mercato, di cui al capo V del Regolamento. Con riguardo a quest'ultimo profilo, se astrattamente il CRA potrebbe contribuire all'*enforcement* di obblighi volti alla tutela dei diritti fondamentali, di cui ad altri atti di diritto dell'Unione, la sua concreta efficacia rimane dubbia, tanto da un punto di vista pratico quanto giuridico.

[*] Assegnista di ricerca in Diritto dell'Unione europea presso il Dipartimento di scienze giuridiche, *Alma Mater Studiorum* – Università di Bologna, virginia.remondino2@unibo.it. Ricerca finanziata dal programma PNRR – Missione 4 istruzione e ricerca – componente 2 dalla ricerca all'impresa, Investimento 1.3, PE0000014 – "*SEcurity and RIghts in the CyberSpace*", finanziato dalla Commissione europea nell'ambito del *NextGeneration EU Programme*.

Keywords: EU *Cyber Resilience Act* (Regolamento UE sulla ciberresilienza) – Diritti fondamentali – Valori dell'UE – Carta dei diritti fondamentali dell'Unione europea – Autorità di vigilanza del mercato

1. Introduzione

Negli ultimi anni, l'incidenza delle minacce e degli attacchi informatici è considerevolmente aumentata, tanto a livello europeo quanto a quello globale [1]. Tra la seconda metà del 2023 ed il primo semestre del 2024, secondo l'Agenzia dell'Unione europea per la cybersicurezza (ENISA), si sarebbe infatti assistito ad una "notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences" [2]. Attacchi informatici che acquisiscono rilevanza non solo in termini quantitativi, ma anche qualitativi, caratterizzandosi per una sempre più spiccata "sofisticazione" [3]. In un mondo estremamente digitalizzato e interconnesso, in cui numerosi individui abbracciano ogni giorno un'esistenza "*onlife*" [4], le minacce informatiche impattano così non soltanto sul tessuto economico, industriale e commerciale, ma anche sulla tutela delle libertà e dei diritti fondamentali riconosciuti in capo ai singoli [5].

---

[1] WORLD ECONOMIC FORUM, *Global Cybersecurity Outlook 2025*, 2025.

[2] ENISA, *ENISA Threat Landscape*, 2024.

[3] Così già P.G. CHIARA, *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in *Rivista italiana di informatica e diritto*, 2023, vol. 5, n. 1, pp. 143-153. Per una panoramica riguardante lo scenario attuale dei principali rischi di cybersicurezza nell'Unione, si veda ENISA, *2024 Report on the State of Cybersecurity in the Union*, 2024.

[4] L. FLORIDI (ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Springer, Cham, 2015.

[5] Cfr. A. DALAL-R. ROY, *Cybersecurity and privacy: balancing security and individual rights in the digital age*, in *Journal of Basic Science and Engineering*, 2021, vol. 18, n. 1, pp. 205-223; M. DUNN CAVELTY-C. KAVANAGH, *Cybersecurity and human rights*, in B. WAGNER-M.C. KETTEMANN-K. VIETH-DITLMANN-S. MONTGOMERY (eds), *Research Handbook on Human Rights*

Non sorprende dunque che già la prima strategia adottata dall'Unione europea (UE) sulla cybersicurezza chiariva come quest'ultima "può essere solida ed efficace solo se si basa sui diritti e sulle libertà fondamentali sancite dalla Carta dei diritti fondamentali dell'Unione europea e sui valori costitutivi dell'Unione" [6]. Un approccio, questo, abbracciato anche dalla più recente "Strategia dell'UE in materia di cibersicurezza per il decennio digitale" [7], in cui il rafforzamento dei livelli di sicurezza informatica viene considerato un elemento essenziale per salvaguardare i diritti e le libertà fondamentali. Ciò in quanto, ad oggi, la cybersicurezza costituirebbe "parte integrante della sicurezza degli europei" [8], i quali "devono avere la garanzia di essere protetti dalle minacce informatiche" [9] derivanti dall'utilizzo di servizi e prodotti, tra cui i dispositivi connessi presenti sul mercato interno.

Invero, nel contesto di un quadro normativo che ha recentemente subito una significativa evoluzione [10], l'esigenza di garantire la cybersicurezza dei prodotti *hardware* e *software* ha trovato terreno fertile nel Regolamento 2024/2847 sulla ciberresilienza ("*Cyber Resilience Act*", "CRA" o "Regolamento") [11]. Quest'ultimo, adottato dal Parlamento europeo e dal Consiglio nell'ottobre del 2024, stabilisce specifici requisiti per i c.d. "prodotti con elementi digitali" [12] (PED) messi a disposizione sul mercato interno, indipendentemente dal loro luogo di produzione.

Caratterizzandosi come uno strumento giuridico i cui effetti non sono quindi prettamente domestici, il CRA mira a definire (internamente) i requisiti a cui i

---

and Digital Technology. Global Politics, Law and International Relations, Edward Elgar, Cheltenham, 2025, pp. 70-93.

[6] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013), 1 final (in prosieguo Strategia per la cybersicurezza 2013), p. 4.

[7] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020), 18 final (in prosieguo Strategia per la cybersicurezza 2020).

[8] *Ibid.*, p. 1.

[9] *Ibid.*

[10] Per un'esaustiva panoramica, si rimanda al contributo di F. CASOLARI-F. FERRI-S. VILLANI, *La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea*, in questo volume, pp. 27-50.

[11] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza).

[12] Ai sensi dell'art. 3, n. 1, CRA, i PED consistono in "qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente".

menzionati prodotti devono conformarsi per poter essere commercializzati sul territorio dell'Unione, nonché a promuovere (esternamente) tali *standard*, sulla scorta del noto "effetto Bruxelles" [13] ed in linea di continuità con altri atti adottati dall'Unione in ambito digitale [14]. In questo modo, il CRA tenderebbe, almeno in astratto, all'affermazione della sovranità tecnologica (o digitale) europea [15] a livello internazionale, "ritagliando" all'Unione il ruolo di attore digitale globale [16].

La dimensione extraterritoriale del CRA assume rilevanza ai fini della presente analisi, per due ragioni. In primo luogo, come già messo in luce dalla prima strategia dell'UE sulla cybersicurezza, anche oltre i confini dell'Unione "gli Stati possono abusare del ciberspazio per sorvegliare e controllare i propri cittadini. L'UE può combattere questa situazione *promuovendo la libertà in linea e garantendo il rispetto dei diritti fondamentali online*" [17]. In secondo luogo, ai sensi dell'art. 3, par. 5, e dell'art. 21, par. 2, lett. a), TUE, l'Unione è tenuta a rispettare e promuovere i suoi valori [18], compresa la tutela dei diritti fondamentali, anche con riguardo agli "aspetti

---

[13] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2019.

[14] Tra gli atti recentemente adottati dall'Unione, si menzioni *inter alia* il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (in prosieguo "*AI Act*" o "Regolamento sull'intelligenza artificiale"). Criticamente sul punto, cfr. M. ALMADA-A. RADU, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, in *German Law Journal*, 2024, vol. 25, n. 4, pp. 646-663.

[15] Per riflessioni su tale nozione, vedasi *ex multis* L. FLORIDI, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy & Technology*, 2020, vol. 33, pp. 369-378; S. POLI-E. FAHEY, *The strengthening of the European Technological Sovereignty and its legal bases in the Treaties*, in *Eurojus*, 2022, n. 2, pp. 147-164; G. FINOCCHIARO, *La sovranità digitale*, in *Diritto pubblico*, 2022, n. 3, pp. 809-827; S. YAKOULEVA, *On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows*, in *Legal Issues of Economic Integration*, 2023, vol. 49, n. 4, pp. 339-348; N.A. SMUHA, *Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective*, in G. BARRETT-P. MÜLLER-GRAFF-J. RAGEADE-V. VADÁSZ (eds), *European Sovereignity: the Legal Dimension*, Springer, Cham, 2024, pp. 127-149.

[16] Così E. FAHEY, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford University Press, Oxford, 2022.

[17] Strategia per la cybersicurezza 2013, p. 3.

[18] *Ex* art. 2 TUE, i quali, come noto, ricomprendono il rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze.

esterni" [19] delle diverse politiche dell'UE, tra cui il mercato interno [20].

Le ragioni che hanno guidato la Commissione a presentare la proposta di Regolamento sono molteplici [21]. Da una prospettiva strettamente giuridica, il CRA mira ad arginare il rischio di un "mosaico legislativo" [22] derivante dai diversi atti adottati sia a livello UE [23] sia a quello nazionale [24]. Strumenti che, secondo la Commissione, affronterebbero in maniera limitata e parziale i rischi di cybersicurezza, creando "incertezza del diritto" [25] per i venditori e gli utilizzatori dei menzionati prodotti. In secondo luogo, il *Cyber Resilience Act* si propone di assicurare il corretto funzionamento del mercato interno, creando le condizioni per lo sviluppo di prodotti *hardware* e *software* sicuri, immessi cioè sul mercato senza (o con limitate) vulnerabilità.

Infine, ma non per ordine di importanza, il Regolamento contribuirebbe a migliorare la tutela dei diritti e delle libertà fondamentali, salvaguardando in particolare il diritto alla *privacy* e alla protezione dei dati personali, nonché la libertà di impresa ed il diritto di proprietà [26], rispettivamente consacrati agli artt. 7, 8, 16 e 17 della Carta dei diritti fondamentali dell'Unione europea (la "Carta"). La proposta di Regolamento coglierebbe così alcune considerazioni formulate nel corso delle consultazioni dei portatori di interesse, i quali avevano sottolineato come "[a]n increased level of cybersecurity for ICT products as well as increase the understanding among users about such level of cybersecurity would be consistent with the Charter" [27]. Da una prospettiva analoga,

---

[19] Art. 21, par. 3, TUE.

[20] Sul rispetto dei valori nell'ambito dell'azione esterna dell'Unione, vedasi *inter alia* M. CREMONA, *Values in EU Foreign Policy*, in M. EVANS-P. KOUTRAKOS (eds), *Beyond the Established Orders: Policy Interconnections between the EU and the Rest of the World*, Oxford University Press, Oxford, 2011, pp. 275-316.

[21] V. Relazione che accompagna la proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, COM(2022), 454 final (in prosieguo proposta di CRA).

[22] *Ibid.*, p. 4.

[23] Si pensi, in via esemplificativa, alla normativa in materia di responsabilità per danno da prodotti difettosi. V. Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi.

[24] Ad esempio, il sistema di etichettatura per i dispositivi "*Internet of Things*" (*IoT*) introdotto in Finlandia nel 2019 e la c.d. "etichetta di sicurezza" per determinati prodotti connessi adottata dalla Germania.

[25] Proposta di CRA, p. 4.

[26] *Ibid.*, p. 9.

[27] Wavestone, CEPS, CARSA, ICF, *Study on the need of Cybersecurity requirements for ICT*

il Comitato economico e sociale europeo, nel proprio parere riguardante la "normativa sulla ciberresilienza", evidenziava come il CRA potesse "consentir[e] ai cittadini/consumatori di beneficiare di una migliore protezione dei loro diritti fondamentali quali la privacy" [28].

Prendendo le mosse da queste premesse, lo scritto intende analizzare il contributo offerto dal *Cyber Resilience Act* alla tutela dei diritti fondamentali dell'Unione europea, come suggerito, in particolare, dalla Commissione nella proposta di Regolamento. A questo fine, si esaminerà in primo luogo l'approccio "securitario-valoriale" adottato dall'Unione nella definizione delle norme in materia di cybersicurezza dei prodotti con elementi digitali, come emerge dallo studio dei documenti di *policy* (par. 2). Successivamente, si analizzerà se, ed eventualmente in quale misura, tale approccio ha trovato concretizzazione nel *Cyber Resilience Act*, soffermandosi su due distinti profili: l'impianto sistemico del CRA e la definizione dei requisiti essenziali di cybersicurezza dei prodotti con elementi digitali (par. 3), nonché le norme in materia di vigilanza del mercato (par. 4). Saranno infine formulate alcune considerazioni conclusive (par. 5).

2. L'approccio dell'UE alla cybersicurezza dei prodotti con elementi digitali: l'affermazione del paradigma securitario-valoriale

L'approccio dell'Unione europea alla cybersicurezza dei prodotti con elementi digitali ha subito, nel corso degli ultimi anni, una significativa evoluzione. Se la prima strategia adottata dall'Unione in materia di cybersicurezza nulla prevedeva in proposito – salvo evidenziare, in termini generici, come i prodotti *hardware* e *software* prodotti nell'UE e in paesi terzi debbano risultare affidabili e sicuri, nonché garantire la protezione dei dati personali [29] – successivi documenti di *policy* hanno messo in luce la doppia "anima" che contraddistingue, ad oggi, la definizione delle norme sulla cybersicurezza dei prodotti connessi.

Tale paradigma – che potremmo definire di natura "securitaria-valoriale" – emerge chiaramente dalle conclusioni del Consiglio dell'Unione europea sulla

products—No. 2020-0715: Final Study Report, in https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products, 2021, p. 82.

[28] COMITATO ECONOMICO E SOCIALE EUROPEO, *Parere del Comitato economico e sociale europeo sulla Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, 2023/C 100/15*.

[29] Strategia per la cybersicurezza 2013, p. 13.

cybersicurezza dei dispositivi connessi del 2 dicembre 2020 [30]. In esse si chiarisce infatti come, al fine di accrescere la fiducia nel mercato digitale, sia necessario rafforzare la "resilienza" [31] dei prodotti presenti sul mercato interno, garantendo al contempo la centralità dei valori dell'UE [32].

Da un lato, pertanto, le norme in materia di cybersicurezza dei prodotti connessi costituiscono una *conditio sine qua non* per sostenere il corretto funzionamento delle reti, dei servizi essenziali e delle infrastrutture critiche situate sul territorio dell'Unione, rafforzando, in ultima istanza, la sicurezza del mercato interno dalle minacce e dagli attacchi informatici. Chiara sul punto è la menzionata strategia dell'UE in materia di cybersicurezza per il decennio digitale, la quale riconosce come "[c]on la diffusione dell'Internet delle cose, è necessario rafforzare le norme applicabili, *sia per garantire la resilienza complessiva che per aumentare la cibersicurezza*" [33]. Sotto questo profilo, la Strategia è coerente con altri atti di *soft law* adottati dall'Unione, tra cui la strategia dell'UE per l'Unione della sicurezza [34], la nuova strategia industriale per l'Europa [35] e la risoluzione del Parlamento europeo sulla strategia dell'UE in materia di cybersicurezza per il decennio digitale [36].

Dall'altro lato, l'approccio dell'Unione alla definizione delle norme in materia di cybersicurezza dei prodotti con elementi digitali tenderebbe alla salvaguardia

---

[30] CONSIGLIO DELL'UNIONE EUROPEA, *Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi*, 2020.

[31] Sebbene il termine "resilienza" sia ricorrente nel contesto dell'azione dell'Unione in materia di cybersicurezza, né il *Cyber Resilience Act* né i numerosi documenti di *policy* adottati dalle istituzioni dell'Unione in tale ambito ne forniscono una definizione univoca. In dottrina, il termine è stato concettualizzato come "the preparedness of organisations against and ability to recover after cyber-attacks". Così I. KAMARA, *European Cybersecurity Standardisation: a Tale of Two Solitudes in View of Europe's Cyber Resilience*, in *Innovation: The European Journal of Social Science Research*, 2024, vol. 37, n. 5, pp. 1441-1460, p. 1442. Sul legame tra cybersicurezza e resilienza, si veda altresì I. LINKOV-A. KOTT, *Fundamental Concepts of Cyber Resilience: Introduction and Overview*, in I. LINKOV-A. KOTT (eds), *Cyber Resilience of Systems and Networks*, Springer, Cham, 2019, pp. 1-25; E. LONGO, *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, pp. 203-234, p. 208. In questo volume, si veda, R. BRIGHI, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica*, pp. 9-26.

[32] *Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi*, cit., punto 1.

[33] Strategia per la cybersicurezza 2020, p. 10, enfasi aggiunta.

[34] COMMISSIONE EUROPEA, *Sulla strategia dell'UE per l'Unione della sicurezza*, COM(2020), 605 final, in particolare p. 3.

[35] COMMISSIONE EUROPEA, *Una nuova strategia industriale per l'Europa*, COM(2020), 102 final, in particolare pp. 14-15.

[36] PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo del 10 giugno 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale*, (2021/2568(RSP)).

e alla promozione dei valori di cui all'art. 2 TUE, rappresentando questi ultimi, come risaputo, "*l'identità stessa* dell'Unione europea" [37]. La Strategia sulla cybersicurezza del 2020 tende in questo modo a sostenere "un modello politico e una visione del ciberspazio fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici" [38]. Ciò si rifletterebbe, in particolare, nella definizione di *standard* di cybersicurezza "values-based". Da questo punto di vista, la Strategia in esame sembra aver influenzato la successiva strategia dell'UE in materia di normazione, che riconosce il potenziale delle norme, anche in ambito *cyber*, quali strumenti atti a proteggere i valori fondamentali posti alla base dell'ordinamento giuridico dell'Unione [39].

L'enfasi posta dalle Istituzioni sulla dimensione "valoriale" dell'azione dell'Unione in materia di cybersicurezza dei prodotti con elementi digitali non deve però sorprendere, per due ragioni. Da un lato, già le precedenti Strategie adottate dall'UE in tema di *cybersecurity* attribuivano un ruolo di rilievo al rispetto dei diritti fondamentali e, più in generale, dei valori dell'Unione, da salvaguardare sia nel mondo digitale, che in quello fisico [40].

Dall'altro, sulla scorta del processo di "costituzionalizzazione" [41] che sta attualmente "plasmando" la transizione tecnologica europea, tale approccio risente indubbiamente del paradigma c.d. "etico-valoriale" e "antropocentrico" proprio dell'azione dell'UE in ambito digitale, quale emerge, ad esempio, dalla comunicazione "Plasmare il futuro digitale dell'Europa" [42], dalla decisione 2022/2481 che istituisce il programma strategico per il decennio digitale

---

[37] Così corte giust. 16 febbraio 2022, C-156/21, *Ungheria c. Parlamento e Consiglio*, punto 127; corte giust. 16 febbraio 2022, C-157/21, *Polonia c. Parlamento e Consiglio*, punto 145; e corte giust. 5 giugno 2023, C-204/21, *Commissione c. Polonia*, punto 67. Si vedano altresì le conclusioni presentate dall'Avvocato Generale Ćapeta il 5 giugno 2025 nella causa C-769/22, *Commissione c. Ungheria*, punto 158. Enfasi aggiunta.

[38] Strategia per la cybersicurezza 2020, p. 22.

[39] COMMISSIONE EUROPEA, *Una strategia dell'UE in materia di normazione. Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, COM(2022), 31 final, p. 6.

[40] V. Strategia per la cybersicurezza 2013, p. 4; COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017), 450 final, in particolare p. 2.

[41] G. DE GREGORIO, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 2021, vol. 19, n. 1, p. 41; O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: a Road Towards Digital Constitutionalism?*, Hart Publishing, Oxford, 2021; F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *Il Diritto dell'Unione Europea*, 2022, n. 2, pp. 277-326.

[42] COMMISSIONE EUROPEA, *Plasmare il futuro digitale dell'Europa*, COM(2020), 67 final.

2030 [43], nonché dalla Dichiarazione europea sui diritti e i principi digitali per il decennio digitale [44]. Articolando la propria azione attorno al rispetto dei valori dell'Unione, quest'ultima pone perciò l'individuo al centro del processo di regolamentazione, con l'obiettivo di sviluppare una "tecnologia al servizio delle persone" [45].

Questa prospettiva, come anticipato, sembra aver guidato il legislatore dell'UE anche nella redazione del *Cyber Resilience Act*, la cui Proposta, avanzata dalla Commissione europea, evidenziava come, attraverso un intervento normativo di tipo orizzontale [46], il CRA potesse contribuire al rispetto dei diritti e delle libertà fondamentali riconosciuti in capo agli individui [47].

3. Il *Cyber Resilience Act* alla prova dei valori: l'impianto sistemico del CRA e la definizione dei "requisiti essenziali di cybersicurezza"

Delineato l'approccio che caratterizza la strategia dell'Unione in materia di cybersicurezza dei prodotti con elementi digitali, occorre ora esaminare se, ed eventualmente in quale misura, il *Cyber Resilience Act* dia effettiva concretizzazione, tramite le sue disposizioni, alla dimensione "valoriale" del descritto paradigma.

Ad una prima analisi, il testo del CRA sembra dedicare limitata attenzione al rispetto e alla promozione dei valori dell'Unione: il termine "valori" è infatti del tutto assente dal testo del Regolamento, mentre l'espressione "diritti fondamentali" ricorre unicamente in tre occasioni [48]. Ciò rappresenta un elemento di discontinuità rispetto ad altri atti recentemente adottati dall'Unione nell'ambito della sua agenda digitale. Ad esempio, il Regolamento 2022/2065 sui servizi digitali [49] menziona i "diritti fondamentali" trentaquattro volte, una cifra che

---

[43] Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022 che istituisce il programma strategico per il decennio digitale 2030.

[44] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale 2023/C 23/01.

[45] COMMISSIONE EUROPEA, *Plasmare il futuro digitale dell'Europa*, cit., p. 2.

[46] Sul punto, si rimanda al contributo di P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il Cyber Resilience Act*, in questo volume, pp. 153-174.

[47] Proposta di CRA, spec. p. 9.

[48] V. considerando n. 51 e n. 111, nonché art. 57, CRA. Pur non menzionando espressamente i "diritti fondamentali", il considerando n. 32 del Regolamento enfatizza come i requisiti essenziali di cybersicurezza definiti dal CRA "dovrebbero (…) contribuire a migliorare la protezione dei dati personali e della vita privata delle persone".

[49] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022

sale a novantasette nell'ambito del Regolamento 2024/1689 sull'intelligenza artificiale.

Sul piano sostanziale, la limitata attenzione prestata dal *Cyber Resilience Act* al rispetto dei diritti fondamentali, e dunque alla dimensione "valoriale" del paradigma, emerge dall'esame dei requisiti di cui all'art. 6 del Regolamento. Questi ultimi rappresentano gli *standard* [50] a cui i prodotti con elementi digitali devono uniformarsi al fine di poter circolare liberamente nel mercato interno, ai sensi dell'art. 4 del CRA. Nello specifico, si prevede che: (i) i PED devono soddisfare i requisiti essenziali di cybersicurezza di cui all'allegato I, parte I, del Regolamento, posto che essi "siano correttamente installati, siano oggetto di un'adeguata manutenzione e siano utilizzati conformemente alla loro finalità prevista o in condizioni ragionevolmente prevedibili e, se applicabile, siano stati installati i necessari aggiornamenti di sicurezza" [51]; e (ii) i processi adottati dai fabbricanti devono essere conformi ai requisiti di cui all'allegato I, parte II, del Regolamento.

Ebbene, i "requisiti essenziali di cybersicurezza" di cui al menzionato allegato I attribuiscono limitato rilievo alla tutela dei diritti fondamentali, riguardando unicamente la tutela del diritto fondamentale alla protezione dei dati personali di cui all'art. 8 della Carta. Il riferimento è, segnatamente, alla specificazione secondo cui i PED devono trattare solo i dati, compresi quelli di natura personale, che siano "adeguati, pertinenti e limitati a quanto necessario in relazione alla finalità prevista del prodotto con elementi digitali", nel rispetto del principio di minimizzazione dei dati *ex* art. 5, par. 1, lett. c), del Regolamento generale sulla protezione dei dati personali[52]. Inoltre, i PED devono poter proteggere la riservatezza [53] e l'integrità [54] dei dati personali, nel momento in cui questi sono conservati, trasmessi o altrimenti trattati.

Oltre a ciò, gli ulteriori requisiti essenziali di cybersicurezza propri del CRA

---

relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (in prosieguo DSA).

[50] Spetterà alle organizzazioni europee di normazione (*i.e.*, CEN, CENELEC e ETSI), di natura privata, elaborare tali requisiti tramite norme armonizzate, sulla base della richiesta presentata dalla Commissione. V. COMMISSIONE EUROPEA, *Commission implementing decision of 3.2.2025*, C(2025), 618 final.

[51] Art. 6, lett. a), CRA.

[52] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (in prosieguo GDPR).

[53] Allegato I, parte I, par. 2, lett. e), CRA.

[54] Allegato I, parte I, par. 2, lett. f), CRA.

si concentrano strettamente sulla dimensione "securitaria" del paradigma esaminato. Per esempio, si prevede che i PED siano "messi a disposizione sul mercato senza vulnerabilità sfruttabili note" [55], garantiscano che le vulnerabilità possano essere corrette per mezzo di aggiornamenti di sicurezza [56], e siano "progettati, sviluppati e prodotti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di attenuazione dello sfruttamento adeguati" [57]. Presentano una valenza strettamente tecnica e securitaria anche i c.d. "requisiti di gestione delle vulnerabilità" di cui alla parte II dell'allegato I del Regolamento [58].

Ne consegue quindi che, per quanto attiene ai requisiti essenziali di cybersicurezza, il CRA sembra dar forma, principalmente, alla dimensione "securitaria" del paradigma illustrato, con scarsa attenzione alla tutela dei diritti fondamentali. Questa conclusione pare trovare conferma da una più ampia analisi del Regolamento, che guarda, in generale, al suo impianto sistemico. In primo luogo, la scelta della base giuridica dell'Atto, *i.e.* il solo art. 114 TFUE [59], conferma la natura del CRA quale strumento squisitamente di mercato interno [60], non essendo fondato su altre base giuridiche di rilievo per la tutela dei diritti fondamentali, come è invece avvenuto nel caso del Regolamento sull'intelligenza artificiale [61].

Ma vi è di più. La specifica declinazione dell'approccio basato sul rischio [62]

---

[55] Allegato I, parte I, par. 2, lett. a), CRA.

[56] Allegato I, parte I, par. 2, lett. c), CRA.

[57] Allegato I, parte I, par. 2, lett. k), CRA.

[58] Si prevede, ad esempio, che i fabbricanti di prodotti con elementi digitali debbano mettere in atto specifiche politiche di "divulgazione coordinate" delle vulnerabilità, nonché effettuare "prove e riesami efficaci e periodici della sicurezza del prodotto con elementi digitali". V. Allegato I, parte II, n. 5 e n. 3, CRA.

[59] La legittimità dell'art. 114 TFUE quale base giuridica per gli atti di diritto derivato dell'UE inerenti alla cybersicurezza è stata confermata dalla Corte di giustizia dell'Unione europea nella sentenza corte giust. 2 maggio 2006, C-217/04, *Regno Unito c. Parlamento e Consiglio*. V. sul punto Y. MIADZVETSKAYA-R.A. WESSEL, *The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox*, in *European Papers*, 2022, vol. 7, n. 1, pp. 413-438, pp. 418-421.

[60] Sull'utilizzo dell'art. 114 TFUE quale base giuridica del *Cyber Resilience Act*, si rimanda a D. DIVERIO, *Le misure di armonizzazione dell'Unione europea in materia di cibersicurezza: profili istituzionali e basi giuridiche*, in *Eurojus*, 2025, n. 3, pp. 17-37.

[61] L'*AI Act* trova la propria base giuridica negli artt. 114 e 16 TFUE, quest'ultimo riguardante il diritto fondamentale alla protezione dei dati personali. Per una riflessione sulla doppia base giuridica di questo regolamento, precedente alla sua adozione, si rimanda a A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO-F. DONATI-A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione – Vol. 1*, il Mulino, Bologna, 2022, pp. 127-164.

[62] Sul punto, si veda P.G. CHIARA, *Gli approcci regolatori del regolamento UE in materia di*

adottata dal *Cyber Resilience Act* pare confermare la mancata attenzione del Regolamento alla salvaguardia dei diritti fondamentali, in particolare se rapportato ad altri atti recentemente adottati dall'UE nella sfera del digitale. Infatti, nel suddividere i prodotti con elementi digitali in tre categorie di rischio (prodotti di *default*, prodotti con elementi digitali importanti e prodotti con elementi digitali critici), il CRA guarda al rischio che tali beni potrebbero generare, soprattutto, in termini di sicurezza del mercato [63], senza alcun esplicito riferimento al possibile impatto negativo sui diritti fondamentali degli individui. Questo, come anticipato, diversamente da altri atti dell'UE in cui l'approccio basato sul rischio affonderebbe, almeno in via teorica, le proprie radici proprio nella salvaguardia dei valori dell'Unione [64].

Si pensi, ad esempio, al menzionato *AI Act* che, nel classificare i sistemi di intelligenza artificiale in quattro specifiche categorie di rischio [65] definisce quest'ultimo come "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso", danno che può riguardare non soltanto la sicurezza e la salute della persona, ma anche i diritti fondamentali riconosciuti in capo ad essa [66]. In questo modo, il Regolamento sull'intelligenza artificiale vieta quei

---

(cyber)sicurezza dei prodotti: il Cyber Resilience Act, in questo volume, pp. 153-174, pp. 161-164.

[63] Ad esempio, ai sensi dell'art. 7, par. 2, *Cyber Resilience Act*, per essere qualificato come "prodotto con elementi digitale importante", la "funzionalità principale" dello stesso deve rientrare in una delle categorie di prodotti di cui all'allegato III del CRA. Si tratta, in particolare, di prodotti che: (i) svolgono "principalmente funzioni essenziali per la cibersicurezza di altri prodotti, reti o servizi, tra cui la sicurezza dell'autenticazione e dell'accesso, la prevenzione e il rilevamento delle intrusioni, la sicurezza dei terminali o la protezione della rete" e/o (ii) presentano "una funzione che comporta un rischio significativo di avere effetti negativi in ragione della sua intensità e capacità di perturbare, controllare o danneggiare un gran numero di altri prodotti o la salute, la sicurezza o l'incolumità dei suoi utenti attraverso la manipolazione diretta, come una funzione centrale di sistema, compresi la gestione della rete, il controllo di configurazione, la virtualizzazione o il trattamento dei dati personali".

[64] Di questo avviso G. DE GREGORIO-P. DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, vol. 59, n. 2, pp. 473-500.

[65] Ossia: sistemi a rischio inaccettabile, a rischio alto, a rischio limitato e a rischio minimo.

[66] Per commenti sulla declinazione dell'approccio basato sul rischio di cui al Regolamento sull'intelligenza artificiale, anche precedenti alla sua adozione, cfr. M. ALMADA-N. PETIT, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?*, RSC Working Paper 2023/25, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4308072; M. EBERS, *Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU's AI Act*, in *European Journal of Risk Regulation*, 2024, pp. 684-703; S. VILLANI, *Luci ed ombre degli strumenti di tutela dei diritti nell'architettura dell'AI Act basata sul rischio*, in F. LUNARDON-E. MENEGATTI (a cura di), *I nuovi confini del lavoro: la trasformazione digitale*, Italian Labour Law e-Studies, Bologna, 2024, pp. 131-151.

sistemi di IA che pongono in essere un rischio inaccettabile per la tutela della dignità umana e dei diritti fondamentali [67], mentre stabilisce specifici requisiti – tanto di natura tecnica quanto etica – a cui le altre tipologie di sistemi di intelligenza artificiale, *in primis* i sistemi ad alto rischio, dovranno conformarsi per poter circolare liberamente sul mercato interno.

Un approccio simile, come visto del tutto assente dall'impianto sistemico del *Cyber Resilience Act*, è stato altresì abbracciato dal Regolamento 2022/2065 sui servizi digitali. Senza pretesa di esaustività [68], si ricordi che esso presenta quale obiettivo cardine quello di "contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in *cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo*" [69]. In questo modo, tale regolamento suddivide i prestatori di servizi intermediari in diverse categorie – sulla base della tipologia di prestazione offerta e del numero di destinatari del servizio – a cui corrispondono obblighi man mano più stringenti, anche con riferimento alla salvaguardia dei diritti fondamentali. Ad esempio, i fornitori di piattaforme e di motori di ricerca *online* di dimensioni molto grandi – su cui incombono gli obblighi più rigorosi – sono tenuti ad effettuare una specifica valutazione dei rischi sistemici nell'UE che derivano dalla progettazione o dal funzionamento del loro servizio, anche avendo riguardo agli "eventuali effetti negativi, attuali o prevedibili, *per l'esercizio dei diritti fondamentali*" [70].

Alla luce di quanto precede, il *Cyber Resilience Act* non sembra dunque prestare particolare attenzione alla salvaguardia e promozione dei diritti fondamentali. Tuttavia, come si avrà modo di esaminare nel successivo paragrafo, tali diritti giocano un ruolo (più) centrale in seno al capo V del CRA, relativo alle procedure di vigilanza.

---

[67] Art. 5, *AI Act*.

[68] In dottrina, si rimanda a A. PALUMBO, *Disentangling the horizontalisation of fundamental rights in the Digital Services Act: What obligations for online intermediaries?*, in *MediaLaws*, 2024, n. 2, pp. 100-121.

[69] Art. 1, par. 1, DSA, enfasi aggiunta.

[70] Art. 34, par. 1, lett. b), DSA, enfasi aggiunta.

4. Il ruolo dei diritti fondamentali nelle procedure di vigilanza di cui al capo V del *Cyber Resilience Act*

Seguendo gli orientamenti del c.d. "*new legislative framework*" [71] ed in applicazione del Regolamento 2019/1020 [72], il *Cyber Resilience Act* conferisce in via principale [73] alle autorità di vigilanza del mercato degli Stati membri il potere di assicurarne l'efficace attuazione [74], ponendo in essere requisiti (minimi) di armonizzazione, in linea con l'autonomia procedurale riconosciuta in capo ai suddetti Stati [75].

Tra i diversi compiti affidati alle autorità di vigilanza del mercato, l'art. 57 del CRA assegna ad esse – o, nell'inerzia delle stesse, alla Commissione europea [76] – il potere di domandare agli operatori economici di adottare misure correttive [77] qualora i PED e i processi messi in atto dai fabbricanti, sebbene

---

[71] Per una panoramica nel contesto dell'agenda digitale dell'UE, cfr. S. DU BOISPÉAN-M. MUECK-C. GAIE, *Introduction to the European New Legislative Framework*, in M. MUECK-C. GAIE (eds), *European Digital Regulations*, Springer, Cham, 2025, pp. 1-19.

[72] Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011.

[73] Tale attività di vigilanza viene, in alcuni casi, condivisa con la Commissione europea e con ENISA. Si veda, ad esempio, l'art. 56, par. 3, del CRA, che attribuisce alla Commissione il potere di effettuare una valutazione dei prodotti con elementi digitali ritenuti non conformi al Regolamento.

[74] Art. 52, parr. 1-2, CRA.

[75] Per analisi relative alle procedure di vigilanza del mercato di cui al CRA, precedenti alla sua adozione, si rimanda a P.G. CHIARA, *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction*, in *International Cybersecurity Law Review*, 2022, vol. 3, pp. 255-272, spec. pp. 264-265; Y. ZIRNSTEIN, *Better cybersecurity due to increased regulation? The final European Cyber Resilience Act. The first comprehensive, horizontally applicable approach for more cybersecurity in digital products*, in *Computer Law Review International. A Journal of Information Law and Technology*, 2024, vol. 25, n. 3, pp. 65-72, spec. 70-72.

[76] In particolare, ai sensi dell'art. 57, parr. 7-9, CRA, la Commissione può effettuare una valutazione dei rischi dei PED qualora vi siano motivi per ritenere che tali prodotti presentino i rischi di cui al par. 1 della medesima disposizione, informandone le autorità di vigilanza del mercato competenti. Ciò può avvenire in "circostanze che giustifichino un intervento immediato per preservare il corretto funzionamento del mercato interno", e qualora la Commissione ritenga che le autorità di vigilanza del mercato competenti non abbiano adottato misure efficaci. Sulla base della valutazione effettuata la Commissione, consultando gli Stati membri e gli operatori economici interessati, potrà stabilire, tramite atti di esecuzione, misure correttive o restrittive a livello UE.

[77] Ai sensi dell'art. 57, par. 1, CRA, tali misure possono consistere, ad esempio, nel ritiro o nel richiamo dei PED dal mercato.

conformi al Regolamento, presentino un "rischio di cibersicurezza significativo" [78], nonché comportino un rischio per "la conformità agli obblighi previsti dal diritto dell'Unione o nazionale *a tutela dei diritti fondamentali*" [79]. Tale disposizione, che non conosce corrispettivi nella normativa dell'Unione in materia di sicurezza generale dei prodotti [80], trova il proprio "*regulatory sibling*" [81] nell'art. 82 del Regolamento sull'intelligenza artificiale, ai sensi della quale se un'autorità nazionale di vigilanza del mercato ritiene che un sistema di intelligenza artificiale ad alto rischio, conforme al Regolamento, possa rappresentare "*un rischio* per la salute o la sicurezza delle persone, *per i diritti fondamentali* o per altri aspetti della tutela dell'interesse pubblico" [82], richiede all'operatore economico interessato di adottare misure adeguate.

Ad un più attento esame, però, l'art. 57, par. 1, lett. b), del CRA e l'art. 82, par. 1, dell'*AI Act* presentano, da un punto di vista sostanziale, una differenza degna di nota. Invero, quest'ultima disposizione presuppone un rischio ai "diritti fondamentali" di per sé considerati, in linea con l'economia complessiva del Regolamento sull'intelligenza artificiale [83] e, più specificamente, con gli obblighi posti a tutela dei diritti fondamentali che incombono sui fornitori e sui *deployers* dei sistemi di IA ad alto rischio [84].

Diversamente, l'art. 57 del CRA considera quale parametro per la determinazione del rischio la conformità agli *obblighi* posti a tutela dei diritti fondamentali, derivanti sia dal diritto dell'Unione che da quello nazionale. Tale

---

[78] Art. 57, par. 1, CRA.

[79] Art. 57, par. 1, lett. b), CRA enfasi aggiunta.

[80] Si veda, in particolare, il capo V del Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio.

[81] P.G. CHIARA, *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, in *European Journal of Risk Regulation*, 2025, vol. 16, n. 2, pp. 469-484, p. 481.

[82] Art. 82, par. 1, *AI Act*, enfasi aggiunta.

[83] V. sul punto criticamente M. ALMADA-N. PETIT, *The EU AI Act: between the rock of product safety and the hard place of fundamental rights*, in *Common Market Law Review*, 2025, vol. 62, n. 1, pp. 85-120.

[84] È questo il caso, ad esempio, dell'obbligo gravante sui *deployers* dei sistemi di IA ad alto rischio di condurre, prima del loro utilizzo, una specifica valutazione d'impatto sui diritti fondamentali (*Fundamental Rights Impact Assessment*, *FRIA*), ai sensi dell'art. 27 dell'*AI Act*. Per un'analisi di tale strumento, si rimanda a A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Society Review: The Internatonal Journal of Technology Law and Practice*, 2024, vol. 54, pp. 1-18.

valutazione, dunque, sembrerebbe essere più circoscritta e specifica [85] rispetto a quella prevista all'art. 82 dell'*AI Act*, domandando alle autorità nazionali di vigilanza del mercato di pronunciarsi non su rischi – astratti e non meglio qualificati [86] – ai diritti fondamentali riconosciuti in capo agli individui, bensì sul rispetto (o meno) di obblighi volti a tutelare, attuandoli, tali diritti. Ad esempio, con riguardo alla tutela del diritto fondamentale alla protezione dei dati personali, ciò potrebbe verificarsi qualora un'autorità nazionale di vigilanza del mercato riscontrasse un rischio di violazione del GDPR, quale l'obbligo di trattare i dati personali previo consenso dell'interessato per una o più finalità specifiche [87].

In questo modo, perciò, le autorità di vigilanza del mercato nominate dagli Stati membri *ex* art. 52 del CRA non fungerebbero unicamente da "guardiane" del Regolamento, contribuendo altresì – almeno ipoteticamente – a garantire il rispetto di obblighi volti alla tutela dei diritti fondamentali di cui ad altri atti di diritto dell'Unione. Il CRA sembrerebbe porsi così in linea di continuità con quanto stabilito dalla Corte di giustizia dell'Unione europea ("CGUE" o "Corte") nella sentenza *Meta Platforms e a.* del 4 luglio 2023 [88]. In essa, i giudici di Lussemburgo hanno infatti rilevato la possibilità per un'autorità diversa (*in casu*, l'autorità garante della concorrenza di uno Stato membro) da quella preposta alla vigilanza del GDPR di constatare, nell'ambito dell'esercizio delle sue funzioni, la possibile violazione delle disposizioni di detto regolamento [89]. Questo, però, fermo il rispetto dell'obbligo di leale cooperazione [90] tra le

---

[85] Di questo avviso anche P.G. CHIARA, *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, cit., p. 482.

[86] Cfr. G. MALGIERI-C. SANTOS, *Assessing the (severity of) impacts on fundamental rights*, in *Computer Law & Security Review*, 2025, vol. 56, pp. 1-18. Criticamente sulla valutazione del rischio nel contesto dell'*AI Act*, v. C. NOVELLI-F. CASOLARI-A. ROTOLO-M. TADDEO-L. FLORIDI, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in *Digital Society*, 2024, vol. 3, n. 13, pp. 1-29.

[87] Art. 6, par. 1, lett. a), GDPR. Sull'invocabilità di tale disposizione da parte delle autorità amministrative nazionali, cfr. corte giust. 11 novembre 2020, C-61/19, *Orange Romania SA c. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, punto 21; corte giust. 4 ottobre 2024, C-621/22, *Koninklijke Nederlandse Lawn Tennisbond c. Autoriteit Persoonsgegevens*, punto 13; corte giust. 4 luglio 2023, C-252/21, *Meta Platforms Inc. e a. c. Bundeskartellamt*, punto 29.

[88] Corte giust. 4 luglio 2023, C-252/21, cit. Per commenti, v. P. MANZINI, *Antitrust e privacy: la strana coppia*, in *Quaderni AISDUE*, 2023, n. 10, pp. 196-220; I. GRAEF, *Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment*, in *Maastricht Journal of European and Comparative Law*, 2023, vol. 30, n. 3, p. 325-334.

[89] Corte giust. 4 luglio 2023, C-252/21, cit., punto 62.

[90] *Ex* art. 4, par. 3, TUE. Sul principio di leale cooperazione nel quadro dell'ordinamento

differenti autorità di controllo, le quali saranno tenute a concertarsi al fine di espletare i rispettivi compiti [91]. A questo scopo, è interessante rilevare che il *Cyber Resilience Act* prevede espressamente la possibilità per le autorità di vigilanza del mercato, di cui all'art. 52, par. 1, CRA, di collaborare "all'occorrenza, con le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati" [92], segnatamente mediante la comunicazione a queste ultime "di qualsiasi risultanza pertinente per l'esercizio delle loro competenze" [93].

Ciò posto, emergono però alcune criticità. Da un punto di vista pratico, possono essere avanzati dubbi circa le competenze della autorità di vigilanza del mercato in materia di tutela dei diritti fondamentali, in particolare con riguardo a quei diritti che esulano dall'ambito delle loro tradizionali funzioni (ad esempio, la tutela dei consumatori) [94]. A questo proposito, il CRA non offre una soluzione, prevedendo unicamente che le autorità di vigilanza del mercato degli Stati membri debbano disporre di adeguate risorse tecniche e finanziarie, nonché "umane dotate delle competenze *in materia di cibersicurezza* necessarie per svolgere i loro compiti a norma del presente regolamento" [95], senza però fare espresso riferimento ad *expertise* in materia di tutela delle libertà e dei diritti fondamentali. A fronte di una diffusa carenza di risorse economiche e umane delle autorità di vigilanza del mercato a livello UE [96], pare dubbio che esse riusciranno ad offrire un concreto contributo all'*enforcement* dei menzionati diritti nell'ambito del *Cyber Resilience Act*.

Da una prospettiva prettamente giuridica, invece, ci si può domandare quale sia il ruolo che il CRA conferisce ai soggetti privati titolari dei diritti (fondamentali) che le autorità di vigilanza del mercato mirano a proteggere. In primo luogo, è necessario precisare che il *Cyber Resilience Act* non conferisce alle persone fisiche e giuridiche il *diritto* di presentare un reclamo presso le autorità di vigilanza del mercato, prevedendo unicamente l'obbligo per queste ultime di informare i consumatori sul luogo in cui presentare reclami riguardanti possibili violazioni del Regolamento [97]. In questo senso, quindi, il

giuridico dell'UE, si veda ampiamente F. CASOLARI, *Leale cooperazione tra Stati membri e Unione europea: studio sulla partecipazione all'Unione al tempo delle crisi*, Editoriale scientifica, Napoli, 2020.

[91] Corte giust. 4 luglio 2023, C-252/21, cit., in particolare punti 53-54.

[92] Art. 52, par. 7, CRA. Si veda altresì il considerano n. 32, CRA.

[93] Art. 52, par. 7, CRA.

[94] Art. 38, Carta.

[95] Art. 52, par. 8, CRA, enfasi aggiunta.

[96] P.G. CHIARA, *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, cit., p. 12.

[97] Art. 52, par. 11, CRA. Inoltre, le autorità di vigilanza del mercato sono tenute a fornire ai

CRA si differenzia tanto dal DSA [98] quanto dall'*AI Act* che, nel riconoscere in capo ai soggetti privati la possibilità di esercitare il diritto in parola presso l'autorità di vigilanza del mercato, assegnano un ulteriore strumento di tutela ai singoli [99].

In secondo luogo, nel silenzio del Regolamento, ci si può domandare quali siano i rimedi esperibili dai soggetti privati qualora le autorità di vigilanza del mercato degli Stati membri non effettuino, *ex officio*, la valutazione di cui all'art. 57, par. 1, lett. b), del CRA, cagionando danni ai singoli. A questo proposito si potrebbe, almeno astrattamente, ipotizzare la possibile responsabilità non contrattuale delle autorità nazionali competenti, in applicazione della nota dottrina *Francovich* elaborata dalla Corte di giustizia nell'omonima sentenza [100]. Nondimeno, affinché tale responsabilità si concretizzi, la Corte richiede la sussistenza di tre condizioni cumulative: (i) l'attribuzione, da parte della norma di diritto UE, di diritti ai singoli; (ii) l'esistenza di una violazione grave e manifesta; e (iii) la sussistenza di un nesso di causalità tra tale violazione e il danno subito.

In relazione all'art. 57, par. 1, CRA, sorgono però dubbi circa la sussistenza della prima delle menzionate condizioni e, dunque, dell'effettiva possibilità per i singoli di far valere tale forma di responsabilità in giudizio. Sebbene secondo la Corte i suddetti diritti non sorgano unicamente nel caso in cui le disposizioni di diritto dell'Unione li attribuiscano *expressis verbis* agli individui – ma anche in relazione ad "obblighi positivi o negativi che le medesime impongono in maniera ben definita sia ai singoli sia agli Stati membri e alle istituzioni dell'Unio-

---

consumatori "informazioni su dove e come accedere ai meccanismi per facilitare la segnalazione di vulnerabilità, incidenti e minacce informatiche che possono incidere sui prodotti con elementi digitali". Tale disposizione, assente nell'originale Proposta della Commissione, è stata introdotta dalla posizione del Parlamento europeo definita in prima lettura. V. Risoluzione legislativa del Parlamento europeo del 12 marzo 2024 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)), P9_TA(2024)0130.

[98] Art. 53, DSA.

[99] Nel contesto specifico dell'*AI Act*, infatti, la possibilità di presentare un reclamo presso le autorità di vigilanza del mercato si aggiunge ai rimedi giurisdizionali e amministrativi di cui possono godere i soggetti privati. Cfr. sul punto S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in *Quaderni AISDUE – Fascicolo speciale 2/2024 'L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive'*, 2024, pp. 125-141, p. 128.

[100] Corte giust. 19 novembre 1991, cause riunite C-6/90 e C-9/90, *Andrea Francovich e altri c. Repubblica italiana*. Per un approfondimento, si rimanda a A. BIONDI-M. FARLEY, *Damages in EU Law*, in R. SCHÜTZE-T. TRIDIMAS (eds), *Oxford Principles of European Union Law*, Oxford University Press, Oxford, 2018, pp. 1040-1064, spec. pp. 1048-1053.

ne" [101] – non risulta affatto chiaro quali siano i diritti ad essi "implicitamente" [102] conferiti dall'art. 57, par. 1, del *Cyber Resilience Act*, non attribuendo tale disposizione alcun esplicito diritto agli individui. Infatti, come esaminato, tale norma si limita a disciplinare i casi in cui le Autorità possono domandare agli operatori economici di adottare misure appropriate con riguardo a quei prodotti o processi che comportano rischi specifici, lasciando agli Stati membri un sostanziale margine di manovra in relazione all'effettiva attuazione degli obblighi derivanti dalla disposizione in esame.

Detto ciò, in un'ottica di tutela *ex post*, è bene tenere a mente che i soggetti privati non rimarrebbero privi di mezzi di *enforcement* per far valere il mancato rispetto degli obblighi posti a protezione dei diritti fondamentali di cui all'art. 57, par. 1, lett. b), del CRA. Invero, poiché tale norma non stabilisce nuovi e specifici obblighi ai sensi del *Cyber Resilience Act*, ma rinvia agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali, i singoli potranno continuare a beneficiare dei mezzi di tutela ivi previsti. Ritornando al menzionato esempio della possibile violazione dell'obbligo di trattare i dati personali previo consenso degli interessati, *ex* art. 6, par. 1, lett. a), del GDPR, questi ultimi potranno continuare a disporre dei mezzi di tutela previsti da tale regolamento, tra cui la possibilità di presentare reclami presso le competenti autorità di controllo degli Stati membri, nonché di proporre ricorsi di natura giurisdizionale o amministrativa [103].

5. Conclusioni

In un mondo estremamente digitalizzato ed interconnesso – in cui le minacce e gli attacchi informatici assumono una sempre più spiccata incidenza e sofisticazione – la necessità di garantire la cybersicurezza dei prodotti *hardware* e *software* emerge non solo come un'esigenza di mercato, ma anche quale condizione necessaria per garantire la tutela delle libertà e dei diritti fondamentali riconosciuti in capo agli individui. L'Unione europea, con l'adozione del *Cyber Resilience Act*, ha perciò introdotto specifici requisiti essenziali di cybersicurezza per i prodotti con elementi digitali messi a disposizione sul mercato interno. Questo, come evidenziato, anche al fine di "migliorare in una certa misura la tutela dei diritti e delle libertà fondamentali, come la protezione della vita privata e dei dati personali, la libertà d'impresa e la protezione della

[101] Corte giust. 22 dicembre 2022, C-61/21, *JP c. Ministre de la Transition écologique e Premier ministre*, punto 46.

[102] *Ibid*., punto 47.

[103] Art. 77, GDPR.

proprietà o la dignità e l'integrità della persona" [104], in linea con l'approccio securitario-valoriale abbracciato dall'UE nella definizione delle norme in materia di cybersicurezza dei prodotti connessi.

Ciò posto, la concreta attenzione prestata dal CRA alla protezione dei diritti fondamentali rimane debole. Con riguardo ai profili di tutela *ex ante*, si è evidenziato come i requisiti essenziali di cybersicurezza di cui al Regolamento rispecchino principalmente la dimensione "securitaria" del paradigma, in linea con l'economia generale del *Cyber Resilience Act* e della sua specifica declinazione dell'approccio basato sul rischio. Sotto quest'ultimo profilo, perciò, il CRA segna un punto di discontinuità rispetto ad altri atti recentemente adottati dall'Unione in ambito digitale, ove il c.d. "*risk-based approach*" trova le sue radici proprio nella salvaguardia dei valori dell'UE [105].

Da una prospettiva di tutela *ex post*, invece, si è messo in luce come le autorità di vigilanza del mercato degli Stati membri possono, almeno astrattamente, giocare un ruolo nella tutela dei diritti fondamentali, in quanto l'art. 57, par. 1, lett. b), CRA, conferisce ad esse il potere di richiedere agli operatori economici di adottare misure appropriate qualora i PED e i processi messi in atto dai fabbricanti, sebbene conformi al Regolamento, comportino un rischio per il rispetto di obblighi posti a tutela dei diritti fondamentali, di cui al diritto dell'Unione o nazionale. In questo modo, le menzionate Autorità potrebbero, in astratto, contribuire all'*enforcement* di obblighi volti a proteggere i diritti fondamentali di cui ad altri atti di diritto dell'Unione.

In concreto sorgono però alcune criticità, sia di carattere pratico che giuridico. Con riguardo a quest'ultimo profilo, in particolare, si è sottolineato come il *Cyber Resilience Act* non conferisce ai soggetti privati – titolari dei diritti fondamentali – un espresso *diritto* di presentare reclami dinnanzi alle autorità di vigilanza del mercato di cui all'art. 52 del CRA. Ci si è dunque domandati quali siano i rimedi che potrebbero essere esperiti da tali soggetti qualora le Autorità non pongano in essere, autonomamente, la valutazione di cui all'art. 57, par. 1, del *Cyber Resilience Act*, cagionando danni ai singoli. Se, in via ipotetica, si potrebbe configurare in capo all'Autorità statale una responsabilità per danno non contrattuale, in applicazione della c.d. dottrina *Francovich*, tale possibilità non sembra sussistere in concreto, data la difficoltà di identificare chiaramente i diritti che la norma in questione attribuirebbe, implicitamente, ai singoli. Ad ogni modo, poiché l'art. 57, par. 1, lett. b), CRA, rimanda ad obblighi previsti dal diritto dell'Unione (o nazionale) a tutela dei diritti fondamentali, gli individui potranno continuare a godere dei rimedi previsti da altri atti di diritto UE posti a protezione dei diritti in parola.

---

[104] Proposta di CRA, p. 9.

[105] G. De Gregorio-P. Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, cit.

Capitolo 13

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa

Antonio Pugliese [*], Giulia Lasagni [**]

Abstract: L'affidamento che la società ripone nei sistemi informatici acuisce le preoccupazioni del legislatore, europeo e nazionale, a protezione degli stessi. Incidenti e attacchi possono impattare sulla complessiva tenuta del sistema. Col fine di prevenire e, se del caso, reprimere condotte irrispettose degli interessi in gioco, si aumentano i doveri di adeguamento e, correlativamente, anche i poteri delle autorità di controllo. Ritrovare un equilibrio fra tutela delle esigenze statuali e quelle del singolo sottoposto all'accertamento è opera complessa e lo è ancor di più se, per quegli stessi fatti, ne dovesse derivare un procedimento penale. Con questa consapevolezza, il capitolo, ricostruita sommariamente la legislazione rilevante, si pone l'obiettivo di rintracciare un ideale, nuovo punto di equilibrio.

Keywords: Cybersicurezza – Processo penale – Pubblic private cooperation – Acquisizione dei dati

[*] Assegnista di ricerca in Procedura Penale, Dipartimento di Scienze giuridiche, Università di Bologna, antonio.pugliese7@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU. Pure essendo il capitolo il frutto di una riflessione comune fra gli autori, G. Lasagni è autrice dei paragrafi 3 e 5; A. Pugliese dei paragrafi 1, 2 e 4.

[**] Professoressa Associata di Procedura Penale, Dipartimento di Scienze giuridiche, Università di Bologna, giulia.lasagni6@unibo.it.

1. Introduzione. Cybersecurity, esercizio dei poteri investigativi e responsabilità penale: alcune nuove prospettive

L'attuale crisi politica internazionale, così come alcuni recenti casi giudiziari nazionali e con ampia risonanza nell'opinione pubblica [1], pongono al centro dell'attenzione la tutela degli interessi relativi alla sicurezza informatica e delle reti, quindi della protezione delle infrastrutture. La ragione dei timori connessi alla tutela del cyberspazio è presto spiegata.

La società contemporanea è perennemente interconnessa, affidando alla dimensione digitale una importante fetta delle interazioni necessarie al proprio funzionamento. Anzi, oramai molti ambiti della vita quotidiana hanno piuttosto referenti nella realtà fisica solo in via occasionale, poiché nascono già digitali e in quell'ecosistema si muovono, vengono scambiati e, infine, spesi per gli scopi più disparati.

Tutto ciò ha portato i legislatori a interessarsi ai comportamenti in grado di influire negativamente sulla salvaguardia dei sistemi informatici e sono stati così imposti (qui in termini imprecisi): vasti obblighi di conformità; complesse strutture organizzative di controllo e vigilanza; ampi poteri di ispezione e sanzionatori e numerose forme di cooperazione tra organismi dotati di poteri di vigilanza, non solo a livello nazionale.

A tutela delle infrastrutture informatiche è dispiegato un variegato arsenale e che vede sulla scena non solo l'autorità giudiziaria penale. Un ruolo di primo piano, infatti, è svolto da autorità amministrative: l'Autorità garante per la protezione dei dati personali (qui «Garante» o «Garante privacy») e, ultimo in ordine di tempo, l'Agenzia per la Cybersicurezza Nazionale (di seguito: «ACN»). L'ACN, a sua volta, è attratta in una strutturata rete di interazioni a livello europeo, fondate sul principio di "leale collaborazione" fra Agenzie e corpi di vigilanza.

In questo senso, il settore della cybersicurezza si inserisce appieno nella attuale era di prevenzione collaborativa, un frangente temporale in cui si accrescono i doveri di adeguamento in capo ai soggetti destinatari degli obblighi

[1] Per citarne uno di grande impatto, si pensi alla diffusione di immagini dal contenuto sessualmente esplicito all'insaputa delle malcapitate vittime, ovvero con commenti del tutto inappropriati, per usare un eufemismo.

derivanti dalla normativa di settore e, correlativamente, si moltiplicano le autorità di controllo, con immediato aumento dei loro poteri ispettivi, di vigilanza e sanzionatori.

A fronte di questo orizzonte a tinte chiaro-scure, il presente capitolo analizzerà ciascuno degli ambiti appena citati, alla ricerca di possibili implicazioni che il dispiegamento dei poteri amministrativi di vigilanza può avere nel procedimento penale e di come il ruolo crescente dei privati stia contribuendo a ridisegnare i modelli di accertamento. Sotto questo versante, vanno al tempo stesso considerate sia la severità delle sanzioni previste dalla più recente legislazione in materia di sicurezza informatica, sia il potenziale utilizzo dei dati raccolti durante le operazioni di ispezione e sorveglianza in sede amministrativa (di vigilanza) nel contesto processuale penale, ove alla violazione delle norme di sicurezza si accompagni una condotta perseguibile anche penalmente [2]. La pervasività degli strumenti di controllo riconosciuti all'ACN e alle sue varie componenti operative (ad esempio, il Computer Security Incident Response Team o CSIRT-Italia) pone con forza la questione del rispetto dei diritti dei soggetti

[2] Si tratta di tecnica legislativa non nuovissima, quella di devolvere ad autorità amministrative di vigilanza compiti ispettivi o, per certi versi, latamente investigativi e anche sanzionatori. Anzi, quello della sicurezza informatica è solo l'ultimo dei settori caratterizzati da questa prassi. Volendo citare almeno un altro campo in cui, in Italia, si sperimenta lo stesso approccio, si può pensare alla legislazione antimafia, d.lgs. n. 159/2011 (cfr., per esempio, la c.d. "informazione interdittiva antimafia", art. 84 ss. e, in particolare, l'art. 93).

In dottrina la produzione in argomento è amplissima, sia nel diritto amministrativo, sia in quello penale. Fra i molti contributi, si rinvia al recente V. MANES, *La resistibile ascesa della "prevenzione mite"*, in *Diritto di difesa*, al link: https://dirittodidifesa.eu/wp-content/uploads/2025/07/MANES-LA-RESISTIBILE-ASCESA-DELLA-PREVENZIONE-MITE.pdf; M. ARBOTTI, *Interdittive antimafia e prevenzione patrimoniale non ablativa: tra funzioni manifeste e latenti*, in *Diritto di difesa*, al link: https://dirittodidifesa.eu/wp-content/uploads/2025/08/ARBOTTI-INTERDITTIVE-ANTIMAFIA-E-PREVENZIONE-PATRIMONIALE-NON-ABLATIVA-TRA-FUNZIONI-MANIFESTE-E-LATENTI.pdf. Si veda poi E. BIRRITTERI, *L'eccezionalismo italiano nella lotta al crimine organizzato: vantaggi, insidie e prospettive della prevenzione antimafia "cooperativa"*, in *Arch. pen.*, 1, 2025; G. D'ANGELO-G. VARRASO, *Il decreto legge n. 152/2021 e le modifiche in tema di documentazione antimafia e prevenzione collaborativa*, in *Dir. pen. cont.*, 2, 2022, p. 12 ss.; F. GIACALONE, *Il nuovo volto dell'informazione antimafia dopo le novelle del D.L. n. 152/2021: verso la definitiva consacrazione del "diritto amministrativo dell'emergenza criminale"?*, in *Dir. econ.*, 2, 2023, p. 37 ss.; S. IPPEDICO, *Le interdittive antimafia tra collaborazione e contraddittorio: nuove contraddizioni?*, in *Cass. pen.*, 12, 2023, p. 4337 ss.; F. GIACALONE, *L'influenza eurounitaria sull'espansione del contraddittorio nei procedimenti amministrativi nazionali*, in *Dir. pubbl. europeo*, Rassegna online speciale, 1, 2024, al link: https://iris.unipa.it/retrieve/51266380-fa9f-4555-a262-61f8a8c03703/GIACALONE%20-%20DPE.pdf; M. MAZZAMUTO, *Profili di documentazione amministrativa antimafia*, in *Giust. amm*., 3, 2016. Sia consentito anche il rinvio a A. PUGLIESE-M. ZITO, *L'ultimo volto dell'interdittiva antimafia: una nuova forma di "compliance" amministrativa*, in *Arch. giur. Filippo Serafini*, 4, 2022, p. 967 ss.

sottoposti al controllo nei contesti amministrativi e, non meno importante, della possibile rilevanza e utilizzabilità dei dati così raccolti in eventuali procedimenti penali, qualora l'elemento fosse considerato utile.

Non per ultimo, come già accaduto in altri rami, all'orizzonte appaiono sempre più rilevanti, anche in questo settore, forme di partnership pubblico-private. Ambiti come quello dell'antiriciclaggio e dell'antiterrorismo già lo hanno sperimentato e, fra questi ultimi e quello della cybersicurezza v'è più d'una somiglianza. Su tutte: gli ampi doveri di segnalazione posti in capo ai soggetti sottoposti alla vigilanza delle autorità di settore e che spingono i privati verso nuove soluzioni [3].

Queste, in estrema sintesi, sono le sfide con cui deve rapportarsi anche l'interprete e nel presente capitolo, a seguito di una sommaria ricostruzione normativa – che toccherà i soli lembi legislativi utili all'approfondimento – si analizzeranno le prospettive, i rischi o i vantaggi che si stagliano all'orizzonte di questa lunga era di prevenzione collaborativa.

2. Quadro giuridico dell'UE e italiano in materia di cybersicurezza e Agenzia per la Cybersicurezza Nazionale (ACN): poteri di ispezione e di vigilanza

Alle fondamenta dell'odierno dibattito sulla sicurezza cibernetica, si pone la Direttiva NIS 1 (1148/2016) [4], recepita in Italia con il d.lgs. n. 65/2018 [5]. Non

[3] Sia consentito un rinvio a G. LASAGNI, *Public private partnerships nell'antiriciclaggio e antiterrorismo: una nuova forma di outsourcing del processo penale?*, in *Dir. pen. contemporaneo*, rivista trimestrale, 3, 2021, p. 153 ss. Nello scritto si sosteneva, seppure per altri rami dell'ordinamento, e si è osservata «una crescente tendenza verso l'"esternalizzazione" delle funzioni di accertamento penale, tradizionale dominio della parte pubblica». Su questa stessa lunghezza d'onda, anche M. CAIANIELLO, *Poteri dei privati nell'esercizio dell'azione penale*, Torino, 2003. Per una analisi in ambito comparato, si veda B. VOGEL, *Reinventing Eu Anti-Money Laundering. Towards a Holistic Legal Framework*, in B. VOGEL-J.B. MAILLART (eds), *National and International Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, Intersentia, Cambridge-Antwerp-Chicago, 2020.

[4] Direttiva del Parlamento Europeo e del Consiglio relativa a misure per un elevato livello comune di sicurezza informatica in tutta l'Unione, che abroga la direttiva (UE) 2016/1148. A livello europeo, la cosiddetta direttiva NIS 1 (Dir. UE 1148/2016) è il primo atto legislativo dell'UE in materia di sicurezza informatica. La direttiva ha attuato la prima strategia dell'UE in materia di sicurezza informatica con l'obiettivo di rafforzare la sicurezza delle reti e dei sistemi informativi.

[5] La ricostruzione a seguire sarà mirata ai soli lembi legislativi più rilevanti e necessari per una corretta comprensione dell'argomento e terrà conto dell'attuale panorama legislativo, influenzato

occorre entrare nel merito dell'atto, sia perché non è specifico oggetto del presente contributo, sia in ragione delle evoluzioni legislative recenti, su tutte il recepimento della Direttiva 2555/2022 c.d. NIS 2 (d.lgs. n. 138/2024). Va detto, però, che il d.lgs. n. 65/2018 è stato solo il primo di una serie più articolata di provvedimenti e oggi rimane ancora un referente significativo per diversi dei principi che enuclea.

Oggi, con l'Agenzia per la Cybersicurezza Nazionale (istituita a mezzo del d.lgs. n. 82/2021), i poteri e le funzioni un tempo distribuiti tra diversi Ministeri si vedono confluiti in un unico organismo. Il recente recepimento della Direttiva NIS 2 (*ex* d.lgs. n. 138/2024), aumenta ulteriormente l'insieme delle funzioni preventive, investigative e sanzionatorie di questo organo. Riprendendo la bipartizione già presente nella Direttiva NIS 1, gli operatori di servizi essenziali sono stati invitati ad adottare misure adeguate e appropriate per gestire i rischi associati alla fornitura dei loro servizi, al fine di ridurre al minimo i rischi informatici connessi agli stessi (secondo il cosiddetto principio di minimizzazione del rischio). A questo proposito, è stato posto l'onere su tali operatori di notificare al CSIRT gli "incidenti" con un impatto significativo [6]. In estrema sintesi, si tratta di un quadro normativo che, per fasi, ambisce a coprire le reti e i sistemi informativi (e in ogni fase) da fattori esterni potenzialmente in grado di impattare negativamente sui primi e ciò include: obblighi strutturali, sino a quelli volti a ridurre al minimo i rischi, ovvero agli obblighi di notifica al CSIRT. Inoltre, già prima dei recenti interventi legislativi, il d.lgs. n. 65/2018 aveva conferito significativi poteri di ispezione alle autorità di vigilanza. Pertanto, i sottoposti al controllo potevano e possono incorrere in sanzioni amministrative significative, per le violazioni degli obblighi gravanti sugli stessi e non è escluso che la condotta non costituisca anche un reato, inasprendo ulteriormente il panorama sanzionatorio [7].

Di seguito al d.lgs. n. 65/2018, veniva promulgato il d.l. n. 105/2019, c.d. "Decreto Perimetro". L'atto ha rafforzato, tra l'altro, la risposta sanzionatoria nel settore della cybersicurezza, introducendo le sue violazioni tra quelle che

---

dal recente recepimento della direttiva NIS 2 (n. 2555/2022, per il tramite del d.lgs. n. 138/2024). Inoltre, si vedranno necessari alcuni brevi richiami alla l. n. 90/2024, sul rafforzamento delle infrastrutture informatiche e sull'apporto di modifiche sia al codice penale sia a quello di procedura penale.

[6] In argomento, appare utile la *guida alla notifica degli incidenti al CSIRT-Italia*, reperibile sul sito istituzionale dell'ACN e al link: https://www.acn.gov.it/portale/documents/20119/552690/ACN_Guida_Notifica_Incidenti_CLEAR.pdf/e7a1b3df-fac0-9b10-fb4d-c08be31061ad?t=1722593115655.

[7] Questa prospettiva è testualmente confermata dal d.lgs. n. 138/2024, che recepisce la direttiva NIS 2 e mantiene l'assetto così sommariamente evocato. Si tratta dell'art. 38 del d.lgs. n. 138/2024 e 34 della Direttiva NIS 2.

possono comportare una responsabilità per fatto di reato dell'ente [8]. Tra le disposizioni degne di nota ai fini della presente analisi vi è l'art. 1, commi 11 ss., sempre del Decreto Perimetro, nella misura in cui vengono introdotti delle fattispecie di reato, per coloro che ostacolano le attività di ispezione o di vigilanza (anche su richiesta di dati o metadati) [9].

Disposizioni simili, peraltro, sono stati oggetto di questioni di costituzionalità e legittimità in sede europea, in ambiti di accertamento affini, come quello finanziario (su cui si veda, più compiutamente, il par. 3).

L'ultimo provvedimento legislativo da menzionare è il d.l. n. 82/2021, che istituisce l'Agenzia Nazionale per la Cybersicurezza (ACN). Il decreto chiarisce il significato di "sicurezza informatica" nell'ambito dell'ordinamento giuridico italiano, ovvero «l'insieme delle attività (…), necessari[e] per proteggere le reti, i sistemi informativi, i servizi informatici e le comunicazioni elettroniche dalle minacce informatiche(…)». Gli obiettivi delineati rivestono notevole importanza e interesse per i massimi livelli di governo, in particolare per le responsabilità assegnate alla Presidente del Consiglio dei Ministri (o alla sua autorità delegata) e al Comitato Interministeriale, che la Presidente del Consiglio dei Ministri continua a presiedere. L'Agenzia è responsabile della salvaguardia della sicurezza e della resilienza nel cyberspazio, della prevenzione e della mitigazione del maggior numero possibile di attacchi informatici e della promozione del raggiungimento dell'autonomia tecnologica.

2.1. Gli incidenti cibernetici, gli obblighi di notifica e il potere investigativo di ACN

Cruciale nel sistema è quindi la definizione del concetto di «incidente». Stando alla definizione che ne dà la Dir. NIS 2 (art. 6) è «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi». Rientrano nelle «gestione degli incidenti», sempre secondo l'art. 6, «le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e riprendersi da esso». Al verificarsi di un incidente e, fra tutti, in presenza di «incidenti che hanno un impatto significativo» (art. 23 NIS 2, c.d. incidente significativo, e art. 25, d.lgs. n. 138/2024), sorge l'obbligo di segnalarli [10]. Prendono piede da questa segnalazione tutta una

[8] Intervenendo anche sul d.lgs. n. 231/2001 (art. 24-*bis*, comma 3).

[9] Citati anche nel d.lgs. n. 231/2001 (sempre art. 24-*bis*, comma 3).

[10] L'art. 25 del d.lgs. descrive come segue cosa debba intendersi per incidente significativo, ed è «considerato [tale] se: a) ha causato o è in grado di causare una grave perturbazione

serie di doveri d'accertamento in capo alle Autorità variamente interessate, fra le quali un ruolo di spicco va riconosciuto al CSIRT. La segnalazione è poi favorita da un costrutto normativo nient'affatto di agevole definizione, benché non nuovo alle "cronache" normative recenti.

Su tutto, fra i profili maggiormente significativi, il particolarissimo bilanciamento "costi-benefici" enucleato dalla normativa di settore. A scorrere la NIS 2 si intuisce bene l'incentivo alle segnalazioni. Da un lato, se anche se ne dovesse presentare una quando non sarebbe appropriato, non ne deriverebbero effetti pregiudizievoli [11], mentre, al contrario, chi dovesse omettere di segnalare quando invece avrebbe dovuto si espone a sanzioni di significativo impatto. Insomma, accedendo a un usurato parallelismo, si incentiva una medicina difensiva. Non è infatti un caso se, osservando l'ultima relazione annuale di ACN disponibile, tutti i parametri di riferimento siano in forte crescita. Solo ad osservare le notifiche, queste si vedono aumentate su base annua del 28% circa, le comunicazioni ricevuta da CSIRT dell'oltre 80%.

Si tratta di un trend già noto in altri ambiti. Il settore dell'antiriciclaggio ha già dato prova di impennate nelle segnalazioni, tanto che «[p]ur di non incorrere nelle sanzioni previste dalla normativa, sono sempre più numerose le (…) segnalazioni (…), anche in mancanza di adeguate verifiche o approfondimenti. L'uso difensivo delle [segnalazioni di operazioni sospette], altrimenti detto fenomeno degli *umbrella reports* (…)» [12] è talvolta accompagnato da una minore qualità delle "denunzie", ciò che rischia di annacquare il sistema, conducendolo, in alcuni casi, verso una faticosa battaglia contro i mulini a vento [13].

Forse è presto per giungere a soluzioni di questo tipo anche nello specifico ambito della cybersicurezza, ma non lo è abbastanza per non immaginare, in un futuro già alle porte, lo sviluppo di simili problematiche, tipiche di modelli in cui l'azione del privato assume preminenza nell'accertamento [14]. Anche l'opera degli attori pubblici si legherà al successo che i servizi a sostegno della

---

operativa dei servizi (…) b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche (…)». Si tratta di una descrizione che, per quanto vada migliorando nella lett. b) rimane pur sempre ancorata a giudizi di valore e ciò potrebbe suggerire, in via cautelativa, di denunciare anche quando, a ben vedere, non dovesse trattarsi di incidenti significativi.

[11] Vale a dire: sempre meglio una segnalazione in più che in meno.

[12] G. LASAGNI, *Public private partnerships*, cit. p. 157.

[13] Senza fine, come quella de Don Chisciotte nell'omonimo romanzo di Miguel de Cervantes.

[14] L'azione del privato prenderà presumibilmente piede anche dal punto di vista tecnico, per esempio con l'adozione di servizi volti a schermare i dati aziendali da attacchi esterni, ovvero, al tempo stesso, con l'obiettivo di raccogliere, se possibile, elementi utili per l'identificazione del profilo dell'attaccante. Ne sono esempio le tecniche di *cyber deception*. In questa opera, M. LANDOLFI, *Cybersicurezza* e *cyber deception: sfide e prospettive processualpenalistiche*.

sicurezza delle imprese saranno in grado di recare. Di per sé, si tratta di fenomeno del tutto compatibile con le disparate logiche aziendali. Seppure per il tramite di una semplificazione di certo imprecisa, si potrebbe finanche arrivare a dire che non v'è poi troppa differenza tra il lucchetto posto a presidio del cancello di ingresso alla fabbrica e la serie di chiavi informatiche poste a tutela dei sistemi aziendali. Ciò che muta, forse, è il contesto, l'ecosistema in cui i due approcci vanno calandosi. Solo in un caso, il secondo, quella difesa privata si iscrive in un crocevia di poteri statuali (e, ancor prima: interessi).

Il panorama diviene ancor più sfidante ove si consideri che l'art. 25, d.lgs. n. 138, nel declinare l'obbligo di segnalare gli incidenti di sicurezza informatica, ne sottolinea il potenziale collegamento con attività criminali e chiarisce il ruolo del CSIRT-Italia in questo tipo di casi: «[s]e si sospetta che l'incidente significativo sia di natura criminale, il CSIRT Italia fornisce inoltre alla parte notificante indicazioni sulla segnalazione dell'incidente (…)» alle autorità di contrasto (art. 25, comma 8). L'esito di un interessamento così ramificato e diffuso verso il medesimo fatto storico (l'incidente) accende l'interesse del processualista interessato a conoscere della formazione di elementi di prova poi, un giorno, spendibili anche in un futuribile processo penale, quello che dovesse prendere le mosse proprio dalle medesime condotte. Il timore, neppure troppo remoto, è che si dia vita a "un entità investigativa a più teste", il cui impatto può essere più significativo proprio quando si rifletta di far refluire le conoscenze acquisite altrove in possibili processi penali. Ciò rende doverosi i quesiti in punto di compatibilità con una acquisizione extraprocessuale diffusa di questo tipo e la spendita procedimentale del dato [15].

Prima di procedere oltre, dunque, si rende necessario analizzare i poteri di vigilanza che il d.lgs. n. 138/2024 ha riconosciuto all'ACN. L'obiettivo è quello di individuare, nella legislazione applicabile, le interazioni rilevanti tra le indagini amministrative (cioè quelle condotte dall'ACN) e i procedimenti penali, che potrebbero derivare dagli stessi fatti, se questi costituissero anche un reato ai sensi del diritto penale italiano. La domanda persistente è se gli elementi, gli atti, i documenti e le dichiarazioni raccolte dall'autorità amministrativa nel corso dei propri procedimenti – senza le tutele di un processo penale – possano essere utilizzati anche in quest'ultimo [16].

---

[15] Di nuovo, non è affatto un caso se fra i compiti d ACN, come descritti sul sito istituzionale, vi siano anche quelli afferenti alla «gestione rapporti con Autorità Giudiziaria, Polizia Giudiziaria e Direzione Nazionale Antimafia e Antiterrorismo [ciò che] assicura i rapporti di collaborazione (…)».

[16] *Ex* art. 34, d.lgs. n. 138/2024, «[l]'Autorità nazionale competente NIS monitora e valuta il rispetto da parte dei soggetti essenziali e dei soggetti importanti degli obblighi previsti (…), svolgendo attività di vigilanza attraverso: a) il monitoraggio, l'analisi e il supporto ai soggetti

Le rinnovate capacità investigative e i poteri sanzionatori, sempre più ampi, richiedono un esame approfondito proprio alla luce del recentissimo d.lgs. n. 138/2024. Il punto di partenza è l'art. 34 ss., che identifica i poteri ispettivi e di vigilanza dell'ACN. In primo luogo, la disposizione specifica i principi generali che regolano i poteri esecutivi dell'ACN: monitoraggio, verifica e ispezioni, adozione di misure di sicurezza e imposizione di sanzioni. Come si può dedurre dalla lettura di tali poteri, essi mostrano un crescente grado di afflittività, che copre l'intera gamma delle possibili attività ispettive, dalla prevenzione alle indagini vere e proprie e, quindi, all'irrogazione delle sanzioni. Questo aspetto chiarisce anche l'importanza di riflettere sulla portata concreta delle prerogative dell'ACN, data la gravità delle punizioni che possono essere irrogate. Inoltre, il terzo comma dell'art. 34 chiarisce la rilevanza dei poteri affidati all'ACN, introducendo i principi di «efficacia, proporzionalità e dissuasività» delle indagini in quella sede svolte. Ne consegue che l'esercizio delle prerogative ispettive si concretizza attraverso attività di una certa rilevanza, che assumono ancora più importanza se si considerano le possibili e non remote implicazioni. Vale a dire che dalle informazioni raccolte durante le indagini amministrative potrebbero emergere indizi di reato e, quindi, anche elementi utili alle indagini penali, che sarebbero così alimentate dai risultati delle ispezioni effettuate durante le indagini amministrative (di vigilanza). La questione diventa più delicata se si considera che alcune delle attività ispettive sono particolarmente invasive, sollevando seri dubbi sul rispetto dei diritti delle persone indagate.

Come ormai comune negli ambiti di accertamento ufficialmente o latamente punitivi, la semantica della legislazione in commento, poi, suggerisce come i legislatori europei e nazionali siano stati ispirati, almeno in parte, anche dal processo penale e dall'effetto dissuasivo solitamente associato alle sanzioni ivi previste. Ne è prova l'art. 34, comma 6, del d.lgs. n. 138, in cui si chiarisce che «[l]e attività e i poteri (…) sono rispettivamente svolti ed esercitati nel rispetto dei diritti della difesa e tenendo conto delle circostanze di ciascun caso (…)».

---

essenziali e (…) importanti; b) la verifica e le ispezioni; c) l'adozione di misure di esecuzione; d) l'irrogazione di sanzioni amministrative pecuniarie e accessorie». La questione ha già dato ampiamente da discutere in settori in parte affini, quali l'antiriciclaggio. Si guardi, ad esempio a Corte cost., ord. n. 117 del 10 maggio 2019 e poi a Corte di Giustizia, (Grande Sezione), 2 febbraio 2021, C-481/19. Numerosi, al tempo, gli interessamenti ermeneutici. Fra questi, A. LOGLI, *Nota a Corte costituzionale, 10 maggio 2019, n. 117*, in *Giurisprudenza commerciale*, 2, 2020, p. 230 ss.; S. CONFALONIERI, *Il nemo tenetur se detegere nel labirinto delle fonti. Riflessioni a margine di Corte Cost., ord. n. 117 del 2019*, in *Riv. trim. dir. pen. cont*., 1, 2020, pp. 108-140; M. ARANCI, *Diritto al silenzio e illecito amministrativo punitivo: la risposta della Corte di giustizia. Nota a CGUE, sent. 2 febbraio 2021, C-481/19, Consob*, in *Sist. pen*., 2, 2021, pp. 73-98; ovvero, sia consentito il rinvio a G. LASAGNI, *La corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la corte costituzionale conferma)*, in *Giurisprudenza commerciale*, fasc. 6, 2021, p. 1177 ss.

L'art. 36 del decreto, inoltre, funge da guida per le ispezioni individuali. La disposizione identifica quali tipi di attività investigative può svolgere l'ACN. Viene quindi chiarito in che modo l'Agenzia può ordinare, nell'ambito di applicazione del decreto: «a) verifiche della documentazione (…); b) ispezioni in loco e a distanza (…); c) richieste di accesso a dati, documenti e altre informazioni (…), indicando lo scopo della richiesta (…)». I poteri conferiti sembrano seguire un principio di tipicità quando si tratta di misure investigative. Tuttavia, data l'ampia portata degli stessi, diventa difficile definire chiaramente i limiti del potenziale coinvolgimento dell'Agenzia [17].

Peraltro, il suo esercizio in concreto può essere influenzato da una serie di fattori, tutti indicati nell'art. 34, comma 6, del decreto e fra i quali vengono in rilievo i presupposti che, aggravando la posizione del soggetto controllato, consentono parallelamente un aumento dei poteri dell'Agenzia. Tra queste circostanze, vanno menzionate quelle connesse a una sorta di recidiva («violazioni ripetute») e quelle connesse alla mancata collaborazione durante l'attività ispettiva («ostacolo alle attività di vigilanza (…)» e «fornitura di informazioni false o gravemente inesatte relative agli obblighi previsti dal presente decreto»). Infine, come regola di salvaguardia, «il livello di cooperazione delle persone fisiche o giuridiche ritenute responsabili dall'autorità NIS competente».

Quest'ultimo passaggio evidenzia diversi aspetti critici che devono essere esaminati. Innanzitutto, è opportuno chiarire in che misura uno scenario di attacco informatico possa costituire anche un'ipotesi di reato, ovvero un caso di responsabilità amministrativa, ma derivante da reato, delle società. Ipotesi penali rilevanti, per essere chiari, potrebbero essere quelle commesse da terzi non collegati alla struttura "sotto attacco". Ciò riflette la logica alla base non solo del d.lgs. n. 138, ma pure della l. n. 90/2024, che ha modificato anche il codice penale, inasprendo o inserendo reati specifici in materia, nessuno dei quali, tuttavia, è di natura colposa. Poiché i delitti contestati sono dolosi, il legislatore intenderebbe punire comportamenti tenuti da soggetti esterni alla compagine o all'amministrazione oggetto di attacco informatico. Tuttavia, come insegna anche l'esperienza con l'art. 615-*ter* c.p. sul tema dell'accesso non autorizzato a un sistema informatico, ciò non costituirà la totalità dei casi possibili. Certamente si verificheranno attacchi compiuti da un "intraneus" alla persona giuridica che appare sotto attacco. Le valutazioni di cui sopra, per ciò solo, però, non

[17] Sul punto, poi, va ulteriormente rimarcata la circostanza che, in una prima fase, queste attività vengono poste in essere in sede amministrativa (di vigilanza). Dalla prospettiva del processo penale, i limiti di criticabilità di un'eventuale azione ispettiva "irregolare" sono davvero stretti e, al massimo, rileverebbero sotto il profilo della violazione del diritto al silenzio. Fuori da ipotesi di questa natura, non parrebbe invocabile una generica e per questo non tassativa (come invece pretenderebbero le invalidità processuali penali) irregolarità acquisitiva, specie se dovesse ricadere su fonti documentali (*infra*, parr. 3.2; 4).

cambiano la fisionomia della legislazione. Quindi, almeno formalmente, sarà comunque richiesta la massima cooperazione a chi, oltre ad essere, in ipotesi, soggetto apicale dell'ente, rischi pure di ritrovarsi indagato [18]. Il contesto così delineato può influire sulla formazione degli elementi istruttori, ampiamente intesi e in ogni sede, favorendone l'emersione anche quando sarebbe lecito che il sottoposto opponesse un rifiuto a collaborare. Se si osserva il fenomeno in altri settori del sistema giuridico, peraltro, l'intuizione sembra confermata.

Alcune brevi osservazioni possono servire a illustrare la realtà così come si presenta oggi all'osservatore interessato a comprendere i punti di contatto fra l'ambito amministrativo e quello penale. Sempre più settori, in cui i rischi sembrano essere numerosi, continuano a orientarsi verso una logica partecipativa nelle procedure di accertamento di natura amministrativa. L'esempio più eclatante – oggi – è la normativa antimafia, il d.lgs. n. 159/2011, come da ultimo modificato dal d.lgs. n. 152/2021 [19]. I punti di contatto con la cybersicurezza sono molti e alcuni accenni sono necessari. In primo luogo, la delicatezza dell'area coperta dalle rispettive discipline. La cybersicurezza pone la sfida di mantenere numerosi interessi, e tutti contemporaneamente: (i) l'ordine costituzionale, di fronte al timore di attacchi dolosi; ma anche (ii) l'ordine economico, a causa della capacità di infiltrarsi in questo e alterarne l'equilibrio e, infine, (iii) i diritti dei cittadini, compreso il diritto alla protezione dei dati personali, esposti nel tumultuoso mondo di Internet, a sua volta afflitto dai temuti attacchi informatici.

Di fronte a queste preoccupazioni, come verrà discusso più dettagliatamente nelle sezioni seguenti, i legislatori europei e nazionali hanno quindi ideato un sistema articolato di prevenzione e controllo, in cui sono coinvolte diverse autorità: l'autorità giudiziaria, l'autorità per la sicurezza informatica e, non per ultimo, l'autorità competente per la protezione dei dati personali.

A tal proposito, appare nuovamente utile un confronto con le norme antimafia. Anche alla luce delle più recenti modifiche alla normativa in materia di lotta alla criminalità organizzata (d.lgs. n. 152/2021), è possibile trarre alcuni spunti utili, sebbene con le dovute distinzioni. Si configura, infatti, una tripartizione

---

[18] Ponendo questioni simili a quelle che già si pongono rispetto all'incompatibilità a testimoniare del "nuovo" rappresentante dell'ente. Si veda art. 44, d.lgs. n. 231/2001 e la dottrina formatasi in merito, tra cui G. VARRASO, *Il "compromesso" delle sezioni unite in tema di costituzione ed esercizio dei diritti difensivi dell'ente "incolpato" nel procedimento*, in *Cass. pen.*, fasc. 1, 2016, p. 73.

[19] Cfr. M. VULCANO, *Le modifiche del decreto-legge n. 152/2021 al codice antimafia: il legislatore punta sulla prevenzione amministrativa e sulla compliance 231 ma non risolve i nodi del controllo giudiziario*, in *Giur. pen. web*, 2021, 11, p. 11; G. D'ANGELO-G. VARRASO, *Il decreto legge n. 152/2021 e le modifiche in tema di documentazione antimafia e prevenzione collaborativa*, cit.; e anche A. PUGLIESE-M. ZITO, *L'ultimo volto dell'interdittiva antimafia: una nuova forma di compliance amministrativa*, cit.

dell'esercizio del potere repressivo in senso astratto, sia in ambito antimafia che in materia di cybersecurity. Se si guarda alla legislazione antimafia, si possono individuare una serie di possibili interventi: in ambito penale, per i comportamenti che sfociano nel reato; in ambito amministrativo, come misura cautelare estrema e con lo scopo di evitare l'infiltrazione criminale nel tessuto economico (la cosiddetta informazione interdittiva antimafia, che ha l'effetto di colpire con una incapacità giuridica temporanea e parziale l'impresa); in ambito preventivo, con riferimento alle misure di prevenzione, la cui competenza spetta tuttavia al giudice penale, sezione misure di prevenzione, e che ha invece il compito di condurre la società fuori dalla palude mafiosa in cui rischia di impantanarsi. È utile notare che i controlli effettuati dall'ACN e i poteri conferitigli dalla legge non sono molto diversi. Anch'essi sono caratterizzati da un collegamento con il processo penale ogni volta che si verifica un reato; sono caratterizzati da ampi poteri preventivi, esercitati attraverso attività di monitoraggio e supervisione; e, non da ultimo, da reali poteri repressivi in ambito amministrativo anche attraverso il ricco e severo sistema sanzionatorio. Questa breve sintesi delinea il rapporto tra le indagini in campo amministrativo, le questioni di cybersicurezza e le loro potenziali implicazioni procedurali penali, sulle quali si tornerà nel par. 4.

La questione deve riguardare l'identificazione del momento oltre il quale sarebbe necessario acquisire prove che abbiano già la garanzia del codice di procedura penale. E ancora, occorre riflettere attentamente sulla funzione repressiva delle sanzioni che possono essere imposte dall'ACN nei casi in cui il soggetto controllato eluda o non collabori alle ispezioni. Ciò può porre la parte controllata di fronte a un difficile bivio, già emerso in altri settori: collaborare e rischiare di testimoniare contro se stessi o non collaborare e affrontare sanzioni più severe?

Ciò, però costituisce solo una faccia della medaglia. L'altra attiene a ciò che accade puramente nella sede amministrativa ma che, di nuovo, in un futuro, potrà pure avere rilevanza per un accertamento penale. La prevenzione collaborativa, come si diceva, non è solo nel rapporto tra controllore e controllato, ma pure fra le Autorità coinvolte, nel contesto europeo, dalla tutela dei sistemi informatici e, non per ultimo, nei possibili rapporti funzionali che potranno crearsi con le realtà private.

3. Raccolta e scambio di dati e informazioni nelle attività di vigilanza: tra public-private partnerships e cooperazione fra Autorità. Introduzione

Si tratta di un tema fra i più sfidanti dell'intera disciplina e comprende almeno due versanti di ricerca. Il primo emerge direttamente dalla legislazione di

settore e riguarda la cooperazione tra le numerose autorità astrattamente coinvolte nel campo della cybersicurezza. Il secondo, invece, seppure immediatamente non percepibile [20], risulta essere l'esito prevedibile delle pretese che l'ordinamento oggi pone in carico ai privati interessati dell'adeguatezza cibernetica: una cooperazione pubblico-privata anche ai fini investigativi.

Le due tipologie di cooperazione mantengono una fisionomia ben distinta, almeno in principio, e possono pure condurre a considerazioni di diversa natura. Quella fra autorità, per esempio, pone oggi sfide significative soprattutto con riguardo alle possibili triangolazioni fra i molteplici organi che, nei singoli Stati membri, assicurano il rispetto della legislazione eurounitaria nell'ambito della sicurezza dei sistemi informatici. Da un lato, ciò pone questioni sulla efficacia delle forme di cooperazione; dall'altro, più il sistema è efficace, più si rischia di esacerbare la asimmetria informativa fra autorità pubbliche e soggetti sottoposti ad accertamento – il che, quando l'accertamento lambisce o si tramuta in indagine penale, è ovviamente un versante alquanto sensibile. Nel caso della cooperazione pubblico-privata, invece, i principali dubbi riguardano innanzitutto la opportunità di stabilire forme di partenariato pubblico-privato che, come si dirà, sempre più si identificano in forme di esternalizzazione di attività di indagine.

Le differenti prospettive consigliano di trattare separatamente i due volti della medaglia.

3.1. Cooperazione fra le autorità

In merito alla cooperazione tra autorità, questa va intesa come almeno di due tipi: (i) interna al singolo ordinamento e fra organismi impegnati in ambiti apparentemente diversi ma accomunati da alcuni scopi comuni di vigilanza; (ii) esterna al singolo Stato e calata in un più ampio contesto europeo o internazionale.

In entrambi i casi, il principio guida di settore si rinviene nell'art. 14 [21] del d.lgs. n. 138, il quale elenca la gamma di possibili coordinamenti tra chi sia potenzialmente incaricato di "investigare" sugli attacchi informatici e delinea un particolarissimo scenario per le aree amministrative interessate dalle ispezioni, alludendo a un complesso meccanismo di sorveglianza, con diversi attori

[20] O nascosto nelle maglie della NIS 2, al Considerando n. 55, ai sensi del quale «[i] partenariati pubblico-privato (PPP) nell'ambito della cibersicurezza possono fornire il quadro appropriato per lo scambio di conoscenze (…). I PPP possono sfruttare le competenze dei soggetti del settore privato per assistere le autorità competenti nello sviluppo di servizi e processi all'avanguardia, compresi, lo scambio di informazioni, i preallarmi, le esercitazioni su minacce e incidenti informatici, la gestione delle crisi e la pianificazione della resilienza».

[21] Non solo questa norma. Si vedano anche, ad esempio, gli artt. 15, 17, 18, 20, 39.

coinvolti. Ciò modella in modo specifico i connotati del sistema, che finisce per rassomigliare – anche solo sul piano interno – a un cane a tre teste: l'ACN con il suo braccio operativo, il CSIRT; la magistratura e, non da ultimo, l'Autorità garante per la protezione dei dati personali [22].

È fondamentale ricordare che, ai sensi dell'art. 15 del d.lgs. n. 138, il CSIRT Italia può instaurare rapporti di cooperazione con i team nazionali di risposta agli incidenti informatici di paesi dell'UE. Nell'ambito di tali rapporti di cooperazione, questo organo «facilita uno scambio di informazioni efficace, efficiente e sicuro con [i] CSIRT nazionali (…), utilizzando i protocolli di condivisione (…). Il CSIRT italiano può scambiare informazioni rilevanti con i team nazionali di risposta (…) di paesi terzi (…), compresi i dati personali (…)».

Si delineano quindi, nella normativa di settore, una serie di nuovi equilibri, che ancora non trovano, spesso, adeguati riscontri in ottica processuale. L'ordinamento interno, infatti, si è perlopiù interessato di normare l'afflusso di elementi utili e raccolti in sede amministrativa di vigilanza, ma non si è ancora spinto sino ad immaginare, dalla prospettiva di una indagine penale, di potere eventualmente acquisire elementi raccolti secondo uno schema "diagonale" di collaborazione fra autorità penali e autorità amministrative di settore e di diverse nazioni [23].

In linea tendenziale, pertanto, quando un procedimento penale deve alimentarsi anche di elementi probatori esteri, lo fa secondo schemi tendenzialmente orizzontali e che, a seconda dei casi, si poggiano o sulle norme in tema di rogatoria, oppure, in ordine ad attività investigative europee, all'Ordine Europeo di Indagine; con l'unica eccezione, limitata però al suo ristretto ambito di azione, del meccanismo di cooperazione diagonale in cui si muove l'Ufficio europeo per la lotta antifrode (OLAF) [24].

Più specificamente, da un lato, la norma generale cui tipicamente si demanda il compito di disciplinare il contatto fra accertamenti in sede amministrativa e

---

[22] *Ex* art. 14, comma 2, d.lgs. n. 138/2024, «[a]i fini della cooperazione e della collaborazione (…) l'Autorità nazionale competente NIS coopera con il Garante per la protezione dei dati personali (…) nei casi di incidenti che comportano violazioni di dati personali (…)».

[23] Va subito precisato che ciò non significa che non vi siano, o non vi possano essere, dei protocolli fra autorità relativi allo scambio di informazioni; qui si intende solo dire che il codice di rito italiano non interviene in punto di regola acquisitiva di documenti che la P.A. italiana dovesse ricevere da altra amministrazione europea, per poi venire introitata in un procedimento penale italiano.

[24] Sull'argomento, anche a livello della sua effettiva applicazione in altri Stati UE, si vedano i risultati del recente progetto di ricerca FACILEX (sito: https://site.unibo.it/facilex/en), i cui risultati sono compendiati in G. LASAGNI-M. CAIANIELLO-G. CONTISSA, *Facilitating Judicial Cooperation in the EU A Computable Approach to Mutual Recognition in Criminal Matter*, Brill, 2024, al link: https://brill.com/edcollbook-oa/title/70688?srsltid=AfmBOorfB5gDZpGu7ZIqs0hDtRGE382P8DnylL26QzmPk945vm0aHyzu.

indagini penali, ossia l'art. 220 disp. att. c.p.p. (che si tratterà in seguito, par. 4.), ha pur sempre un ambito territoriale ben definito: si applica entro i confini della Repubblica e non immagina, almeno non come ipotesi generale, di potere applicarsi anche allo scambio di informazioni fra Amministrazioni di più Stati [25].

D'altro canto, le normative di settore, che spesso delineano alcuni tratti dello scambio di informazioni fra autorità (spesso, fra autorità amministrative e penali) sono estremamente eterogenee e raramente si spingono a definire anche profili essenziali come quelli della ammissibilità o utilizzabilità in giudizio. L'ambito della cybersicurezza conferma questa tendenza, con gli artt. 15 e 34 del d.lgs. n. 138 e l'art. 32 della NIS 2, che, appunto, non contengono regole specifiche riguardo l'ammissibilità nel processo penale degli elementi raccolti eventualmente anche a seguito di scambi di informazioni fra amministrazioni di più Stati.

È in questo contesto che l'apporto conoscitivo rappresentato dai "dati", con la loro valenza potenzialmente pluriespressiva (notizia di reato, elemento di prova, prova), mette in crisi i modelli di cooperazione tradizionali. Detto altrimenti, in mancanza di disposizioni esplicite sul tema, i dati raccolti dalle autorità italiane di cybersicurezza possono essere utilizzati se sono stati richiesti legittimamente ad altre autorità europee nell'ambito della cooperazione speciale prevista dal decreto 138?

La risposta sembra essere affermativa, per lo meno alla luce del quadro normativo attuale. Da un lato, nell'ambito di vigilanza amministrativa, lo scambio di informazioni è supportato dalla base giuridica vigente, senza che si pongano particolari questioni in termini di utilizzabilità all'interno di quel contesto.

Dall'altro, naturalmente, molto più problematica è la situazione in cui tali informazioni finiscano in un fascicolo di indagine penale. La pronta disponibilità del dato istruttorio, infatti, lo rende appetibile per l'Autorità giudiziaria e ciò ottimizza le opportunità di indagine per le Procure che dovessero intervenire a seguito dell'interessamento dell'ACN [26].

---

[25] Semplificando, secondo l'art. 220 disp. att. c.p.p. quando nel corso di attività amministrativa di vigilanza dovessero emergere indizi di reato, gli ulteriori elementi di prova dovrebbero essere raccolti secondo le prerogative di cui al codice di procedura penale. La regola di garanzia, però, è ovviamente pensata per le amministrazioni italiane, non potendosi imporre alcun obbligo a quelle straniere. Ne deriva che per le volte in cui si sostenga sempre più una cooperazione trasversale, a livello amministrativo e fra più Stati, maggiori sono i rischi dell'inutilità della disposizione. Diviene sempre più probabile che quegli elementi, nella cooperazione fra autorità amministrative, giunga fino in Italia e, a quel punto, siano acquisiti sotto forma di documenti nell'ambito di una indagine preliminare (penale). Sul punto, par. 4.

[26] G. Lasagni, *Cooperazione amministrativa e circolazione probatoria nelle frodi doganali e fiscali*, in *Dir. pen. cont*., 2015, https://archiviodpc.dirittopenaleuomo.org/upload/1442824408LASAGNI_2015a.pdf.

Al contempo, i meccanismi tradizionali di tutela, come l'art. 220 disp. att. c.p.p. sono spesso di dubbia applicabilità. In primo luogo, potendosi dubitare della eventualità di conferire qualifica di p.g. alla amministrazione che per prima raccoglie i dati (su cui, si veda nel dettaglio in seguito par. 4). In secondo luogo, considerando che, specie nell'ambito di cui si discute, l'emersione di notizie di reato può essere anche successiva alla indagine su un singolo incidente (ad esempio, emergendo solo a seguito del riscontro di una pluralità di attacchi informatici, magari organizzati) – vanificando in radice l'obiettivo del meccanismo previsto dall'art. 220.

A ciò si aggiungono le disposizioni di cui al d.lgs. n. 138/2024 che, avendo carattere speciale, come indicato, non pongono particolari restrizioni alla circolazione delle informazioni raccolte. Peraltro, le stesse coordinate del codice di procedura penale [27] non vietano e, in certa misura, anzi supportano, almeno sul piano testuale, l'acquisizione dei dati comunque detenuti presso le pubbliche amministrazioni italiane, anche se, a loro volta, fossero stati acquisiti per il tramite di una collaborazione interna agli enti amministrativi con i loro corrispettivi esteri.

Diverse disposizioni mostrano difatti una apertura verso la raccolta dei dati, senza prestare eccessiva attenzione al percorso che li ha resi disponibili. A titolo di esemplificazione, muovono in questo senso gli artt. 234 e 234-*bis* c.p.p., così come la serie di disposizioni sui sequestri, che possono essere pure eseguiti presso amministrazioni dello Stato [28]. Un limite, certo non invalicabile, si rinviene nell'art. 242 c.p.p., che suggerisce un onere di traduzione dell'atto redatto in lingua diversa dall'italiano, se e in quanto necessario, ma che difficilmente si può trasformare in una regola di esclusione probatoria vera e propria [29].

Infine, va pure ricordato che, ai sensi dell'art. 235 c.p.p., è sempre ammessa l'acquisizione di documenti costituenti corpi di reato, a prescindere da chi li detenga e non è uno scenario inverosimile in relazione ad accertamenti di questo tipo.

---

[27] Va ammesso che, in relazione alla velocità delle innovazioni in campo informatico, il codice può essere considerato particolarmente risalente e diversi dei temi qui dibattuti non involsero le riflessioni del legislatore processuale del 1988/89. Nel corso del tempo si è tentato di adeguare il codice alle innovazioni imposte dall'avanzare dell'informatica, ma resistono difficoltà ontologiche e gli ultimi approdi in tema di cybersicurezza comprovano l'assunto. Si assiste, verrebbe da dire, ad una "fuga dalle codificazioni", supportata dalla necessità di disporre di una legislazione sempre aggiornata e dalla corrispondente difficoltà all'adeguamento costante di una struttura complessa come un codice (per sua natura un complesso di norme stabili, in teoria).

[28] Per non parlare del caso in cui il dato è conservato da un privato, su cui si veda la disposizione ampia dell'art. 234-*bis*, così come il recente strumento dell'Ordine di produzione europeo.

[29] Cass., Sez. III, sentenza n. 18136 del 14/05/2025, in argomento, ha recentemente affermato come «[a]ltrettanto infondata appare l'ulteriore eccezione di nullità, proposta con riferimento alla mancata traduzione, dal francese, del verbale di accompagnamento (…) è stata la stessa difesa (…) a sottolineare e a lamentare il carattere meramente formale di quella attestazione di regolarità, con ciò dimostrando di aver ben compreso il contenuto dell'atto non tradotto (…)».

Nell'ambito specifico della cybersicurezza, difatti, in ipotesi, la certificazione di un incidente ad opera del CSIRT potrebbe costituire corpo del reato, così come lo costituirebbe se, per ricostruire lo stesso attacco informatico, la stessa autorità abbia richiesto e ottenuto certificazioni analoghe a un ente corrispettivo presente in altro Stato Membro.

In conclusione, guardando alla tendenza del sistema e alla normativa di settore, si può affermare che i verbali delle operazioni dello CSIRT, poste in essere al di fuori del contesto processuale penale, nasceranno in forma documentale; in questa categoria saranno collocati e, presumibilmente, in quanto tali verrebbero acquisiti al procedimento, con buona pace delle perplessità che potrebbero derivare dalle difformità negli standard acquisitivi.

3.2. Cooperazione pubblico privata

Sull'altro fronte, il crescente dovere di adeguamento di quanti siano sottoposti alla legislazione in materia di cybersicurezza, nonché l'altissimo grado di tecnicismo connesso, conduce inevitabilmente gli attori privati, da un lato, ad essere sempre più coinvolti nel processo di accertamento e, dall'altro e di conseguenza, a innalzare il livello di competenze (giuridiche e tecniche).

Il miglioramento delle loro performances è anche direttamente connesso all'evitare di incorrere in sanzioni rilevanti. Come si è osservato (*supra*, parr. 1 e 2), i soggetti sottoposti alla "giurisdizione" dell'ACN debbono dar prova di aver costruito una struttura "resiliente" [30] contro attacchi esterni, ma pure reattiva, ove non si riuscisse a porre freno a fenomeni intrusivi.

In entrambi i casi, è verosimile che, come in altri ambiti, fra cui il già citato AML/CFT, ciò induca il privato a mettere insieme diverse capacità para-investigative, che possano proteggerlo sia dagli attacchi, sia da possibili sanzioni connesse ad eventuali e riscontrate inefficienze.

Si tratta proprio del meccanismo alla base delle Public-Private Partnerships (PPP), sia in ottica preventiva, sia, in modo molto più controverso, repressiva. La cybersicurezza, infatti, è un settore che trova il proprio punto di forza nel naturale affidamento verso i privati di talune attività investigative, in particolare quelle di raccolta di informazioni su possibili attività sospette [31]. Il quesito di

[30] È poi fra i fattori che, già dagli anni '80, ha guidato prima la nascita e poi lo sviluppo delle Public-Private Partnerships. Si veda per questo, S.J. COLLIER-A. LAKOFF, *The vulnerability of vital systems: How critical infrastructure became a security problem*, in M.D. CAVELTY-K.S. KRISTENSEN (eds), *Securing 'the homeland': Critical infrastructure, risk and (In)security*, Routledge, London, 2008, p. 17.

[31] È poi un tema che la NIS 2 affronta direttamente nel Considerando n. 55), auspicandone la loro diffusione. In tema di PPP, più in generale, si veda B. VOGEL, *Reinventing Eu Anti-Money*

fondo, in relazione ai dati di cui le autorità pubbliche dovessero venire a conoscenza per il tramite di queste partnerships, è quindi riassumibile schiettamente in questi termini: si tratta di una via per aggirare le prerogative processuali? [32]

Sul punto, può essere utile anche tracciare una linea di demarcazione ideale fra le tipologie di PPP ipotizzabili, così come ricostruite dalla dottrina. Due vengono qui in rilievo: (i) una preventiva, c.d. compliance PPP e una (ii) puramente investigativa [33].

Circa la prima, che mira a definire meglio i confini del fenomeno illecito, come la definizione di "incidente", bisogna evitare di cadere in un facile fraintendimento: a fenomeni nei fatti diversi non sempre corrispondono differenziate categorie del diritto. Con ciò si intende dire che le azioni a tutela dei sistemi informatici, in certa misura, non sono poi troppo diverse da quelle che un privato pone in essere a tutela della sua persona e dei suoi interessi. Impianti di videosorveglianza, registrazioni di colloqui in presenza, fotografie, allarmi, investigatori privati segnano già molti procedimenti penali, pure trattandosi di dati nati privatamente, altrove e per fini preventivi. Insomma, va detto che la conoscenza privata non è respinta dal processo e anzi, molte volte l'accertamento di penale responsabilità si fonda su elementi "portati" dal privato. Per questa ragione, si farà fatica a impedire l'acquisizione al processo penale di dati e documenti che il privato avrà formato nel corso delle azioni messe in essere per dar seguito a doveri di compliance aziendale oppure per prevenire rischi specifici del settore merceologico considerato [34]. In questa direzione, a ben vedere, si muove il legislatore europeo, nella misura in cui ritiene che questi

---

Laundering. Towards a Holistic Legal Framework, in B. VOGEL-J.B. MAILLART (eds), *National and International Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, Intersentia, Cambridge-Antwerp-Chicago, 2020, p. 881; ovvero, più ad ampio raggio, B. VOGEL-E. KOSTA-M. LASSALLE, *Law of public-private cooperation against financial crime developing information sharing to counter money laundering and terrorism financing*, United Kingdom, 2024.

[32] Si è già detto più volte nel testo ma è bene ripetere che queste valutazioni sono vere nella misura in cui si dovesse poi approdare a un processo penale. Detto altrimenti, è interesse dello scritto comprendere se, per le volte in cui un attacco cibernetico dovesse costituire anche un'ipotesi di reato, gli elementi raccolti nella sede amministrativa siano spendibili in quella penale e, se sì, a quali condizioni.

[33] B. VOGEL, *Reinventing Eu Anti-Money Laundering*, cit.

[34] Resta in disparte la questione della reale libertà del privato di autodeterminarsi nel mettere insieme le azioni di adeguamento richieste dalla normativa. Come si è già notato in altro scritto, «la partecipazione dei privati a questi meccanismi, così come la condivisione di informazioni specifiche, può essere infatti considerata volontaria solo su un piano formale ed astratto. Nella pratica, invece, l'adesione degli operatori finanziari è spesso fortemente condizionata dalla necessità di mostrarsi cooperativi (…)». Così in G. LASAGNI, *Public private partnerships*, cit., p. 158.

meccanismi di cooperazione possano essere sfruttati dalle autorità, anche al fine di facilitare «lo scambio di informazioni, i preallarmi, le esercitazioni su minacce e incidenti informatici, la gestione delle crisi e la pianificazione della resilienza» (considerando 55, NIS 2).

Diverso è il caso delle PPP con finalità investigativa, di fatto richieste o indotte al privato dalle autorità di controllo e riferite a incidenti specifici. Qui la conoscenza da parte degli organi pubblici della possibilità del privato di svolgere delle indagini può fare la differenza sul piano dell'accertamento e presentare profili innovativi e non regolamentati di acquisizione delle informazioni. L'individuazione delle informazioni rilevanti da parte del privato, infatti, certamente costituisce un vantaggio per l'autorità di controllo, che potrebbe risparmiare risorse per perseguire i propri obiettivi.

Tuttavia, la esternalizzazione delle attività di indagine rischia di bypassare tutte le garanzie procedimentali che le autorità di contrasto dovrebbero altrimenti rispettare nella acquisizione delle informazioni (quelle penali ad un livello più alto, quelle amministrative ad un livello minore, ma sempre più assimilabile a quello penale, specie se dotate di poteri punitivi).

In siffatti frangenti, si può quindi seriamente dubitare della compatibilità di simili modelli acquisitivi e della relativa spendita nel contesto processuale penale degli elementi ottenuti, perlomeno se la azione del privato può essere considerata come determinata dalle richieste (dirette o indirette) delle autorità pubbliche. In questo senso, vengono qui in rilievo, nei termini che si vedranno nel paragrafo subito di seguito, l'art. 220 disp. att. c.p.p. e in generale tutte le garanzie procedurali previste per le fasi dell'accertamento.

Diversamente, laddove il privato agisse di propria iniziativa, anche ove strutturasse sistemi misti, preventivi e investigativi, il panorama muterebbe. Possono esserne un esempio alcuni meccanismi a tutela di eventuali accessi abusivi ai sistemi informatici, come per esempio nell'ambito della *cyberdeception* [35]. Si potrebbe pensare a strutture volte ad intercettare il tentativo di accesso, in grado tuttavia di approntare una difesa contro simili fenomeni e capaci anche di raccogliere dati utili per individuare l'attaccante. La relazione tecnica – privata – che dovesse uscire fuori dalla elaborazione dei dati raccolti dal sistema di difesa potrà certamente corredare, in ipotesi, una denuncia e così entrare nel procedimento penale [36].

---

[35] V., in quest'opera, M. LANDOLFI, *Cybersicurezza e cyber deception: sfide e prospettive processualpenalistiche*.

[36] Con il limite delle attività c.d. provocatorie. Detto altrimenti, alcuni sistemi possono finanche "attrarre" possibili attaccanti, fingendosi vulnerabili e invece ingabbiando il soggetto agente. Il tema, peraltro, è stato recentemente affrontato in giurisprudenza, si veda Cass. Pen., sez. II, n. 10934/2024, ove si è affermato, in linea di continuità rispetto a quanto qui sostenuto, che «[i]nfine,

In questa direzione parrebbe muoversi, come si è visto, anche il legislatore europeo, nel Considerando 55 della NIS 2, incentivando forme di cooperazione pubblico-privata a fini preventivi, così allo stato appare nelle maglie della disposizione europea. Il problema, però, è che risalire alle ragioni che hanno spinto all'azione il privato è tutt'altro che un compito facile, specie in sistemi di cooperazione fluidi e ad alto tasso di informalità, che caratterizzano le Public-Private Partnerships.

4. Art. 220 delle norme di attuazione del codice di procedura penale, atti investigativi misti e comparsa degli indizi di reato

Lo si è visto: le attività amministrative hanno un ruolo da "comprimario" nell'accertamento di talune condotte in contrasto con l'ordinamento. Tuttavia, l'azione del cittadino non rimane necessariamente confinata alla sfera dell'illecito amministrativo. Ciò è particolarmente vero se si considerano le ultime frontiere a cavallo tra sicurezza nazionale, cybersicurezza e violazioni penalmente rilevanti.

Sinora si è data ampia prova di come la criminalità informatica sia oggi il confine più sensibile della società contemporanea. Resta da esaminare un tema, quello del confine, non sempre netto, fra accertamento amministrativo e di natura penale.

Il codice di procedura penale contiene una disposizione alla quale vorrebbe delegare il compito di gestire il difficile passaggio delle prove dal quadro amministrativo, dove talvolta vengono inizialmente raccolte, al contesto processale penale.

La norma in questione è l'art. 220 disp. att. c.p.p. All'origine, la disposizione, occupandosi dell'emergere di indizi di reato in procedimenti extra-penali, sembrava in grado di fornire una risposta completa a tutte le istanze di garanzia che interrogavano la dottrina e la giurisprudenza [37]. Sembra tuttavia che non abbia raggiunto il suo obiettivo, almeno stando agli accesi dibattiti che ancora oggi circondano il tema [38].

---

corretta è la soluzione giuridica relativa alla inapplicabilità, al caso di indagini interne condotte nell'ambito di attività ispettive, dell'art. 220 disp. att. c.p.p. Affinché le cautele ivi previste siano applicate, è necessaria (…) la natura pubblicistica del rapporto tra dichiarante ed esercente la funzione (…)».

[37] Cfr. R.E. KOSTORIS, "*Sub art. 220*", in E. AMODIO-O. DOMINIONI (a cura di), *Commentario del nuovo codice di procedura penale, Appendice*, Milano, 1990, p. 74. Cfr. anche, nella giurisprudenza, Corte Cost., n. 86 del 1968; nn. 148, 149 del 1969; n. 248 del 1983; n. 15 del 1986; n. 330 del 1990.

[38] Si veda, di recente, Cass. Pen., sez. III, n. 43996/2023, ovvero Cass. Pen., sez. III, n. n.

D'altra parte, non potrebbe essere altrimenti se si considera che la questione riguarda diversi fronti del procedimento penale, forse i più importanti e rappresentativi: tutela dei diritti della difesa e dell'efficacia repressiva dell'azione penale. La disposizione si muove in un contesto particolarissimo, ove è ad un tempo probabile che alcuni degli atti compiuti dagli organi amministrativi abbiano anche un valore utilizzabile nei procedimenti penali, nel mentre però emergendo degli indizi di reato.

In breve, può accadere che ciò che viene prodotto in un altro ambito (quello amministrativo) abbia, in realtà, anche un certo valore probatorio (in termini impropri, data la fase) in sede penale. L'affermazione precedente può anche riflettere un risultato fisiologico derivante dall'efficacia delle attività di controllo e di vigilanza svolte dai funzionari pubblici [39]. Tuttavia, può anche accadere che il funzionario della PA, nel corso delle ispezioni, si avveda dell'emersione di uno o più indizi, ciò che accende l'interesse del legislatore processuale, interessato a disciplinare il passaggio di fase, senza soluzione di continuità. Diverso resta il caso del procedimento penale postumo rispetto alle attività di vigilanza disposte in sede amministrativa e ove non emergevano indizi di reato (*supra*, par. 3).

La contestualità fra i due accertamenti, in breve, concorre quale elemento di disequilibrio e acuisce l'importanza dei limiti di utilizzabilità degli atti formati in sede amministrativa di vigilanza. L'aspetto che per primo lascia emergere molte preoccupazioni si riconduce alla circostanza in base alla quale le azioni investigative poste in essere in questa sede esulano dalle tutele stabilite dal codice di procedura penale.

L'argomento si presta a molte considerazioni, non tutte esplorabili in questa

---

6594/2016 o ancora Cass. Pen., SS.UU., n. 45477/2001. In ambiti diversi ma affini, T. RAFARACI, *Reati tributari con soglia di punibilità e applicazione dell'art. 220 disp. att. c.p.p.: la Cassazione rimarca i diritti della difesa*, in *Rivista della Guardia di Finanza*, 3, 2015, p. 674, ovvero anche M. GUERNELLI, *Aspetti operativi e processuali dell'attività di p.g. nel nuovo c.p.p.*, in *Arch. nuova proc. pen*., 1991. Sia consentito poi il rinvio a A. PUGLIESE, *Atto di provenienza amministrativa e prova penale*, in *Rassegna dell'Avvocatura dello Stato*, fasc. 1, 2017.

Sul tema specifico, si vedano gli spunti in G. CORASANITI, *Strategie di contrasto al ransomware e nuove frontiere della criminalità informatica*, in *Dir. inform. e infor*., fasc. 1, 2025, p. 19; ovvero L. MAGLI, *La protezione dei dati personali contro i rischi del digitale*, in *Riv. trim. dir. pubbl.*, fasc. 2, 2025, p. 401 e M. MACCHIA-G. SFERRAZZO, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, in *Dir. amm*., fasc. 1, 2025, p. 109.

[39] Quanto si è sin qui scritto testimonia ciò. È qui in discussione un frangente specifico, inerente proprio al passaggio senza soluzione di continuità tra procedimento amministrativo e penale. I differenti casi sono stati invece affrontati prima nel testo e afferiscono, più che altro, al refluire di conoscenze tra procedimenti amministrativi e penali ma quando questi altri si aprano in un secondo momento rispetto ai primi. La distinzione non è così marcata, eppure da ciò passano numerose garanzie.

sede, è perciò necessario circoscrivere il campo d'azione. La questione più urgente è il rapporto tra gli atti cosiddetti misti e le garanzie difensive previste dal codice di procedura penale. Nello specifico, si tratta di esaminare «i limiti che l'ammissibilità di tali [atti] incontra nelle norme relative» [40] alla formazione della prova nel giudizio penale.

Gli atti a finalità mista [41] trovano un punto d'appoggio normativo nell'art. 220 disp. att. c.p.p.: si tratta degli atti prodotti dai funzionari amministrativi in un contesto molto particolare, ovvero quando la loro attività si muove sui confini sottili e non sempre chiaramente visibili tra l'illecito amministrativo e il reato.

Il problema connesso a ciò è immediatamente individuabile. Occorre garantire, con un ragionevole grado di certezza, che le attività svolte dalla P.A. non si muovano in spregio ai diritti di difesa tutelati dal codice di procedura penale e, ancor prima, dalla Costituzione. La questione è tutt'altro che indifferente alle dinamiche di un accertamento penale e (ancora oggi) non ha sempre trovato un'interpretazione unanime nella giurisprudenza [42].

Infatti, l'art. 220 disp. att. c.p.p. identificherebbe di già il momento oltre il quale si dovrebbe ritenere superato il procedimento amministrativo e iniziato quello penale. Esso stabilisce che «quando nel corso delle attività di ispezione o di vigilanza (…) emergono indizi di reato, gli atti necessari per garantire le fonti di prova (…) sono compiuti in conformità alle disposizioni del codice di procedura penale». Ebbene, il punto più critico risiede proprio nell'individuazione del momento in cui un indizio di reato possa ritenersi "emerso". Diversi sono gli interrogativi. Ci si può domandare se, ad esempio, sia necessario attendere che il reato si mostri completamente, ovvero se si debba giungere a potere abbinare al presunto reato una persona determinata (attribuzione soggettiva).

Va osservato che l'intero sistema di garanzie che il codice di procedura prevede deriva dalla risposta a interrogativi come questi, così come la questione dell'ammissibilità in giudizio delle prove raccolte durante la fase amministrativa. Procrastinare eccessivamente il momento a partire dal quale si ritiene che sia emerso un indizio di reato, potrebbe significare indebolire il contenuto delle tutele della difesa. Si ritiene per queste ragioni più in linea con le esigenze del caso, nonché più coerente con la ragion d'essere stessa della norma, fare riferimento a una concezione quasi embrionale del termine, a una mera *possibilità di*

---

[40] R. ORLANDI, *Atti e informazioni della autorità amministrativa nel processo penale*, Giuffrè, 1992, p. 156.

[41] Per l'ampiezza dell'opera, si può rinviare sempre a R. ORLANDI, *Atti e informazioni della autorità amministrativa*, cit.

[42] Ad esempio, Cass. Pen., n. 1973 del 2015 e n. 4919 del 2015.

reato. È quindi plausibile ritenere che l'art. 220 disp. att. c.p.p. sia destinato ad operare quando la «pubblica amministrazione – nelle sue attività di ispezione e vigilanza – viene a conoscenza di un possibile reato» [43].

Va infatti tenuto presente che non tutti gli atti amministrativi sono "ambigui" e, per il momento, dando per scontata la possibilità che l'amministrazione produca solo atti propri, senza che questi tendano necessariamente al penale, si può evitare un malinteso: non a tutti gli atti si applicano le stesse regole di ammissibilità.

Date le premesse di cui sopra, si può procedere a un controllo delle condizioni che i cosiddetti atti misti devono soddisfare per poter essere ammessi al processo, entrando anche nei fondamenti logici della decisione. Sembra opportuno illustrare qui tutti i problemi che, in termini pratici, possono venire alla luce. Si analizzeranno le seguenti categorie: dichiarazioni (da parte di persone che possono essere sospettate di un reato o possibili testimoni), accessi documentali e ordini di cooperazione.

Conviene iniziare con gli atti dichiarativi e, in particolare, con gli atti contenenti le dichiarazioni di coloro che potrebbero diventare, nel corso del processo, prima indagati, poi imputati. Lo scenario è facile da immaginare. Durante un'attività ispettiva, una persona si trova nella posizione di dover "collaborare" con l'Amministrazione, ma così facendo rischia di rilasciare dichiarazioni autoincriminanti. I dubbi che possono sorgere appaiono intuitivi: *quella persona deve essere ascoltata in base alle norme del codice di procedura o è legittimo rimanere al di fuori di esse?* È qui che emerge la necessità di dare una corretta lettura degli "indizi di reato" di cui all'art. 220. Se si aspettasse una *notitia criminis* meglio configurata, si dovrebbe procedere a prescindere dalle garanzie del codice: si applicherebbe ancora il principio *nemo tenetur se detegere*? La risposta alla domanda verrà dalla prassi che si formerà sulle disposizioni precisamente dedicate alla tutela dei sistemi informatici [44]. Nel frattempo, però, si debbono trarre alcune considerazioni intermedie.

Dal punto di vista del codice di procedura penale, gli elementi raccolti dall'ACN si prestano ad essere ricondotti all'art. 234 c.p.p., ovvero alle prove documentali. È il caso del documento che si riferisce a fatti preesistenti al processo penale e formatosi altrove. Da questo punto di vista, la descrizione sembrerebbe applicarsi perfettamente anche ai documenti raccolti dall'ACN durante

---

[43] R. ORLANDI, *Atti e informazioni della autorità amministrativa nel processo penale*, Giuffrè, 1992, p. 156.

[44] Così come in passato, G. LASAGNI, *La corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la corte costituzionale conferma)*, cit., nonché G. LASAGNI, *Prendendo sul serio il diritto al silenzio. Commento a Corte cost. ord. n. 117 del 10 maggio 2019*, in *Dir. pen. cont*., 2, 2020, pp. 135-162.

le attività di prevenzione e intervento a fronte di attacchi informatici. Ad esempio, i dati raccolti durante le attività preventive, che riguardano la necessaria conformità alle normative di settore, potrebbero essere inclusi in eventuali e futuri procedimenti penali relativi a quegli stessi attacchi informatici. Il caso è diverso se i funzionari dell'ACN e/o del CSIRT Italia, definiti come pubblici ufficiali dalla l. n. 90/2024, art. 22, dovessero raccogliere informazioni su persone potenzialmente sospettate di un reato.

In tal caso, ci sarebbero almeno due possibili considerazioni. In primo luogo, sembrerebbe che la NIS 2 e la l. n. 90/2024 abbiano lo scopo di facilitare l'emergere di informazioni (anche) penalmente rilevanti, identificando così una possibile transizione tra attività di vigilanza amministrativa e procedimenti penali. D'altra parte, le dichiarazioni rese da una persona passibile di incriminazione sollevano la questione: (i) del rispetto del diritto di difesa; (ii) dell'attendibilità delle dichiarazioni rese da chi sia interessato a difendersi. In questa prospettiva, infine, non aiuta la disarmonia che emerge dalla normativa NIS 2, secondo la quale la mancanza di collaborazione può essere valutata nell'imposizione della sanzione e tuttavia, secondo il diritto processuale, alla stessa persona andrebbe riconosciuto il diritto di non autoincriminarsi e quindi a non collaborare. Una dicotomia difficile da sanare, aggravata dall'estrema severità delle sanzioni previste dalla disciplina NIS 2, solo in parte mitigata dal considerando n. 131 della Direttiva, che invoca il rispetto del principio del *ne bis in idem*. Frase più che allusiva e che potrebbe anche sottendere alla necessità di non imporre due sanzioni di natura (sostanzialmente) penale, come quelle contenute nella Direttiva e nel decreto di recepimento italiano potrebbero essere catalogate, secondo i principi dettati, tra l'altro, da oramai noti precedenti, quali A. B. c. Norvegia (CEDU) o Menci, Garlsson e De Puma (CGUE) [45], in ossequio agli standard – meglio noti come "criteri" Engel [46]. Da qui, quindi, l'importanza di garantire la piena operatività dell'art. 220 disp. att. c.p.p.

Oltre a ciò, l'attuazione della norma dipende dalla qualifica che può essere attribuita ai funzionari dell'ACN, quando dispiegano i loro poteri di vigilanza. In sintesi, l'ambito di applicazione dell'art. 220 sarebbe ancora più ampio se costoro fossero considerati in grado di sommare funzioni di polizia giudiziaria. Ciò significherebbe che gli stessi funzionari sommerebbero la funzione di polizia giudiziaria al primo emergere di un "indizio di reato", con il conseguente obbligo di acquisire gli elementi probatori, da quel momento in poi, secondo le norme e le garanzie del codice di procedura penale. Altrimenti, in attesa di capire in quale direzione si muoverà la prassi, in tutti i casi, quegli stessi

[45] Corte EDU, nn. 24130/11 e 29758/11. CGUE, caso *Menci* (C-524/15); *Garlsson Real Estate* (C-537/16) e causa *Di Puma* (C-596/16 e C-597/16).

[46] Corte EDU, n. 5100/71, Engel e altri c. Paesi Bassi.

funzionari, espressamente definiti come pubblici ufficiali dall'art. 22, l. n. 90/2024, avrebbero l'obbligo immediato di denuncia.

In ogni caso, tuttavia, data anche la gravità delle possibili sanzioni amministrative (e che si teme possano avere una consistenza penale), il soggetto sottoposto al controllo, aggrappandosi ai criteri Engel [47], avrebbe ugualmente motivi per opporsi a una forma più lieve di collaborazione, o per non collaborare affatto, appellandosi all'esercizio di un diritto e, in particolare, quello di difesa.

La conclusione, allo stato dell'elaborazione in materia, resta di matrice speculativa; eppure, può ritrovare in altri ambiti utili agganci. Le riflessioni sui procedimenti CONSOB, per esempio, hanno restituito, in un passato affatto remoto, ricostruzioni dottrinali e giurisprudenziali degne di nota, mosse dal fine di evitare patenti contorsioni processuali. Le particolarità che possono essere proprie del settore che occupa questo scritto, si rivedono anche nella vicenda che, a su tempo, impegnò la Corte di Giustizia dell'UE [48] e ciò fortifica le conclusioni cui qui si è pervenuti.

Nell'ambito della cybersicurezza il rischio maggiore si ha quando la medesima condotta costituisca sia violazione della disciplina di settore, sia fattispecie incriminatrice. Il rischio, però, è confinato a ipotesi non necessariamente così ricorrenti. Con questo si vuole dire che le varie fattispecie disseminate nel codice penale, o in leggi speciali, e qui di rilievo sono di matrice dolosa. In molti casi il potere ispettivo e sanzionatorio dell'ACN prescinde dal verificarsi di una fattispecie di reato.

Consistenti sanzioni, infatti, si applicano all'ente che dovesse, per esempio, omettere l'obbligo di notifica in caso di incidente, ovvero in caso di scarsa collaborazione ai test che dovessero essere indetti dagli organismi predisposti (art. 1, comma 8, d.l. n. 105/2019, richiamato *ex* art. 24-*bis*, d.lgs. n. 231/2001). Non necessariamente in ognuno di questi casi si deve presupporre l'esistenza di un reato e, soprattutto, seppure dovesse esservi, sono rari i casi in cui l'entità sotto attacco abbia al suo interno un soggetto apicale che, operando da *intraneus* ma contro l'ente che dirige, ad esempio si adoperi per una esfiltrazione dei dati. Sono casi siffatti ad accendere la serie di allarmi evidenziati soprattutto nell'ultimo paragrafo. Negli altri, si tratterà di applicare, grossomodo, quanto esplorato nella

---

[47] G. LASAGNI, *Prendendo sul serio il diritto al silenzio. Commento a Corte cost. ord. n. 117 del 10 maggio 2019*, in *Dir. pen. cont.*, 2, 2020, pp. 135-162.

[48] Di nuovo, per brevità, sia consentito il rinvio a G. LASAGNI, *La corte di giustizia riconosce il diritto al silenzio*, *op. cit*., ove, a p. 1180, richiamandosi alla vicenda, si rammenta come il ricorrente «si era ripetutamente rifiutato di presenziare alle audizioni della Consob e, una volta comparso, aveva opposto alle richieste di informazioni la facoltà di non autoincriminarsi. All'esito del procedimento, l'accusato veniva condannato non solo per la condotta di insider trading, ma anche a norma dell'art. 187-*quinquiesdecies* TUF, per il comportamento poco collaborativo».

parte precedentemente nella trattazione. Come che sia, le modalità operative concesse dalla normativa di settore ampliano l'orizzonte conoscitivo delle pubbliche autorità, anche oltre i confini nazionali e secondo assetti collaborativi che – al netto di resistenze politiche pure ipotizzabili – potrebbero rivelarsi efficaci e questo è un fatto, col quale conviene cimentarsi, potendosi immaginare la sua crescente rilevanza in futuro.

5. Conclusioni

Le considerazioni sopra esposte chiariscono la complessità delle prospettive di fronte alle quali si trova l'interprete quando si tratta di cybersicurezza. È stata compresa l'importanza di dare un significato adeguato all'art. 220 c.p.p., al fine di garantirne l'effettiva operatività.

È chiaro che un'interpretazione estensiva del termine «indizi di reato» si allinea meglio con la logica della norma e le esigenze del sistema. In breve, la condizione di cui all'art. 220 dovrebbe essere considerata soddisfatta ogniqualvolta gli organi investigativi e amministrativi abbiano già raccolto elementi che consentano loro, anche con un margine di dubbio molto ampio, di considerare astrattamente la rilevanza penale di un fatto.

D'altra parte, i "nostri indizi" non solo sono inadeguati a costituire la base di un giudizio di responsabilità, ma possono essere – ed è qui che emerge il carattere marcatamente garantista della norma – anche in riferimento a una possibile incriminazione. Essi devono solo essere in grado di orientare quella che era iniziata come un'indagine amministrativa verso la strada dell'indagine preliminare. Per quanto riguarda la presunta distinzione tra polizia amministrativa e giudiziaria, in termini generali, la distinzione ha senso; ma ha senso fino a quando è soddisfatta la condizione di cui al 220 disp. att. c.p.p. [49].

In definitiva, la scarsa percorribilità della distinzione fra i modelli di accertamento (penale/amministrativo – pubblicistico/privatistico) è sempre riconducibile all'emergere dei suddetti indizi. Una volta raggiunto tale stadio, si verificherebbe una tale commistione di poteri e funzioni che qualsiasi teoria sulla loro diversità avrebbe scarsa credibilità. In conclusione, ci troviamo di fronte a un dilemma finale: fino a che punto si possono anticipare le prerogative del codice? Tutte le analisi e le valutazioni dell'ACN devono attenersi alle prerogative della legge processuale penale? Fino a che punto, ed eventualmente come procedimentalizzare le indagini puntuali svolte dai privati? E come distinguere

[49] Si veda anche F.N. RICOTTA, *Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria*, in *Dir. pen. cont.*, 1, 2023.

i casi in cui il privato agisce quale longa manus dell'autorità e quando invece di propria iniziativa?

La prospettiva di estendere le prerogative codicistiche può apparire allettante, ma occorre meditare attentamente. Se si procedesse in questo modo, si rischierebbe di creare una situazione di ingiustizia non distante da quella che invece si vorrebbe censurare. Si moltiplicherebbero i procedimenti penali, anche quando non necessario, con conseguente aggravio per l'autorità giudiziaria e, dall'altro lato, più individui si vedrebbero costretti a sostenere anche i costi "di immagine" conseguente all'essere iscritto nel registro degli indagati [50]. La distinzione che si è posta, fondata sulle diverse possibili situazioni ipotizzabili, mira a mantenere un ragionevole equilibrio fra le molteplici istanze con cui deve di già cimentarsi l'interprete. Appare oramai innegabile una forte compenetrazione fra l'ambito pubblicistico e quello penale e, vista l'iper-specializzazione di molte materie (quella della cybersicurezza è solo l'ultima [51]), si mostra essere una strada senza ritorno. Il processo penale si alimenterà delle conoscenze che proverranno da altri apparati dello Stato e, più di frequente forse, anche di quelle che dovessero essere messe insieme dai privati.

Nulla di nuovo sotto il sole, entro certi limiti. Ciò detto, infatti, andrà disegnato con cura il perimetro della legittimità delle attività para-investigative poste in essere al di fuori del procedimento penale, onde evitare che in queste si ritrovino escamotage per aggirare le prerogative e le legittime aspettative che – ed è bene ricordarlo – nel codice di rito sono costruite tutte attorno a precetti sovralegali. Quando, invece, le stesse ispezioni in sede amministrativa dovessero tramutare in accertamenti sul fatto costituente reato, in quel momento occorrerà garantire il più rigoroso rispetto dell'art. 220 disp. att. c.p.p.

Su questi precari equilibri si giocherà la futura sfida della cybersicurezza, in bilico tra i poteri dell'ACN e l'autorità giudiziaria. L'obiettivo è trovare un nuovo baricentro, che tuteli i vari interessi: la sicurezza della società nel suo complesso, la salvaguardia dei diritti di ogni individuo all'interno di quella società, compresi coloro che dovessero essere sospettati di aver commesso un reato.

---

[50] Per comune esperienza, se è pur vero che un'archiviazione può "riabilitare" l'immagine dell'indagato, è pur vero che sino a quel momento l'iscrizione fra gli indagati può condurre a conseguenze pregiudizievoli sul piano reputazionale.

[51] Solo a mo' d'esempio, si può pensare alla privacy, al settore ambientale, a quello bancario, all'antiterrorismo e altri esempi vi sarebbero.

Parte IV

Consapevolezza, educazione e politiche

Capitolo 14

Cybersicurezza e fattore umano: un approccio educativo inclusivo

Antonella Carbonaro [*], Enrico Gnagnarella [**]

Abstract: La cybersicurezza contemporanea si basa sia sulle soluzioni tecnologiche sia sul pieno coinvolgimento del fattore umano, riconosciuto oggi come elemento centrale per garantire la protezione dei sistemi digitali. La consapevolezza, le competenze e i comportamenti degli utenti possono rafforzare significativamente la resilienza informatica, mentre errori, disattenzioni e carenze di preparazione restano tra le principali cause di incidenti. Lo stesso fattore umano può diventare una risorsa strategica se adeguatamente formato, coinvolto e responsabilizzato. Questo lavoro analizza le strategie educative più efficaci per rafforzare la resilienza cibernetica attraverso un approccio inclusivo, capace di raggiungere persone di diversa età, ruolo, competenze e background culturale. L'attenzione è rivolta alla progettazione di percorsi formativi accessibili, adattivi e culturalmente sensibili, in grado di tradurre concetti tecnici in esperienze di apprendimento concrete e partecipative. Il rafforzamento delle competenze digitali, l'etica nell'uso delle tecnologie e l'adozione di comportamenti sicuri diventano così i pilastri di una cultura condivisa della sicurezza. L'analisi si completa con esempi di buone pratiche provenienti da ambiti pubblici, aziendali ed educativi, dimostrando come un investimento mirato sul fattore umano possa ridurre i rischi informatici e promuovere una cittadinanza digitale più consapevole e responsabile.

Keywords: Cybersicurezza – Fattore umano – Educazione digitale – Formazione inclusiva e continua – Consapevolezza informatica – Etica digitale

---

[*] Professoressa associata confermata, Dipartimento di Informatica – Scienza e Ingegneria, Università di Bologna, antonella.carbonaro@unibo,it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

[**] Assegnista di ricerca SERICS, Dipartimento di Informatica – Scienza e Ingegneria, Università di Bologna, enrico.gnagnarella2@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

1. Introduzione

La componente umana è spesso considerata sia un punto debole sia una risorsa potenziale nella sicurezza informatica, in quanto gran parte degli incidenti cyber ha origine da errori o comportamenti umani. Il rapporto CLUSIT [1] conferma che la maggioranza degli attacchi riusciti è stata facilitata da sviste o configurazioni errate da parte di utenti e operatori IT. Secondo il *Data Breach Investigations Report di Verizon* [2], tre violazioni su quattro coinvolgono un errore umano come causa primaria. Questi dati evidenziano come tecniche di social engineering sfruttino le vulnerabilità umane per penetrare sistemi altrimenti robusti. In Italia, la carenza di sensibilizzazione alla sicurezza digitale si manifesta ancora attraverso comportamenti a rischio, come la tendenza a cadere vittima di tentativi di phishing, segnalando una significativa mancanza di consapevolezza [3]. In sintesi, i comportamenti e le decisioni di ciascun utente possono influire direttamente sulle vulnerabilità di un sistema informatico e persino determinare il successo di un attacco [4]. Di contro, lo stesso fattore umano può diventare un pilastro di resilienza cibernetica se adeguatamente formato e coinvolto. Lo sviluppo di una solida *cultura della sicurezza* trasforma l'utente da punto debole a prima linea di difesa. La consapevolezza diffusa delle

[1] CLUSIT – ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA, *Rapporto Clusit 2025: cybersecurity in Italia e nel mondo – Security Summit di marzo 2025*, Clusit, 2025.

[2] VERIZON COMMUNICATIONS, *Data Breach Investigations Report 2025*, Verizon, 2025.

[3] AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN), *Strategia Nazionale di Cybersicurezza 2022-2026*, 2022.

[4] AICA MONDO DIGITALE, *Il fattore umano e la regolazione della cybersecurity*, 2022.

minacce quotidiane e l'adozione di buone pratiche (es. gestione password, riconoscimento di e-mail fraudolente, backup dei dati) è riconosciuta come elemento fondamentale per proteggere sia sé stessi sia l'organizzazione [5]. In altri termini, investire sul fattore umano significa accrescere la cyber resilience complessiva: personale vigile e competente può prevenire incidenti, rilevare tempestivamente anomalie e reagire in modo appropriato agli attacchi, mitigandone gli impatti. Pur rimanendo inevitabilmente un rischio, l'errore umano può essere drasticamente ridotto attraverso educazione, formazione e responsabilizzazione degli utenti. Riconoscere il ruolo centrale dell'elemento umano richiede un approccio multidimensionale alla cybersecurity, che oltre alla tecnologia consideri fattori psicologici, organizzativi e sociali.

2. Strategie educative inclusive per la cybersicurezza

Promuovere una cultura cyber solida richiede strategie formative inclusive, capaci di raggiungere pubblici eterogenei e tenere conto delle diverse necessità quali abilità, età e background culturali. La sicurezza digitale deve entrare a far parte delle competenze di cittadinanza di tutti, non solo degli specialisti, attraverso programmi educativi accessibili e adattabili. In quest'ottica, l'educazione alla cybersecurity va resa inclusiva, coinvolgendo tanto gli addetti ai lavori quanto i dipendenti non tecnici e il grande pubblico, con strategie su misura per ciascun gruppo. Di seguito si delineano alcuni princìpi e approcci chiave per una formazione cyber inclusiva.

2.1. Accessibilità e diversità cognitiva

Un approccio inclusivo parte dall'accessibilità dei contenuti formativi: materiali, corsi e piattaforme devono essere fruibili anche da persone con disabilità sensoriali o cognitive. Questo implica, ad esempio, progettare video con sottotitoli e audio-descrizioni, utilizzare linguaggio chiaro e visualizzazioni intuitive, e offrire alternative testuali per chi ha difficoltà con i media audiovisivi. La diversità cognitiva suggerisce inoltre di impiegare metodologie didattiche varie per adattarsi a differenti stili di apprendimento. Un'attenzione specifica va posta a non sovraccaricare gli utenti con gergo tecnico: concetti di sicurezza complessi dovrebbero essere spiegati con esempi concreti e metafore comprensibili, così da risultare di facile utilizzo anche ai non specialisti. Rendendo il design

[5] ACN & DIPARTIMENTO PER L'INFORMAZIONE E L'EDITORIA, *Accendiamo la cybersicurezza. Proteggiamo le nostre imprese. Campagna di sensibilizzazione*, 2024.

della formazione cyber universale, si abbattono le barriere all'apprendimento e si permette a un pubblico più vasto di acquisire nozioni di base sulla sicurezza informatica.

2.2. Eterogeneità dei destinatari (ruoli, età e background)

Le campagne di sensibilizzazione efficaci riconoscono che non esiste un solo profilo di utente, ma molteplici. Occorre quindi personalizzare i contenuti formativi in base ai diversi ruoli professionali, fasce d'età e livelli di esperienza digitale dei destinatari [6]. Ad esempio, i programmi per dirigenti e decision-maker enfatizzeranno gli aspetti di governance del rischio e di compliance, mentre per i dipendenti operativi punteranno su procedure pratiche quali gestione sicura di password, riconoscimento di phishing, uso corretto degli strumenti aziendali. Analogamente, nelle scuole occorre personalizzare i messaggi in base all'età: agli studenti più giovani si insegneranno i concetti base tramite strumenti educativi come giochi o storytelling, mentre a studenti più grandi si possono proporre simulazioni di attacchi e laboratori pratici. Anche all'interno di un'azienda, un approccio inclusivo prevede moduli differenziati: formazione di base per tutto il personale, approfondimenti tecnici per team IT e sessioni specifiche per figure apicali. L'approccio basato sul pubblico, evidenziato anche da ENISA come buona pratica, massimizza la rilevanza dei contenuti e quindi l'efficacia dell'apprendimento [7]. Importante è inoltre tenere conto del pregresso di ciascuno: chi ha scarse competenze digitali va guidato passo-passo, evitando assunzioni di conoscenze, mentre utenti avanzati possono essere sfidati con esercitazioni più complesse.

2.3. Diversità culturale

In società sempre più multiculturali, i programmi di educazione alla cybersecurity devono essere sensibili alla diversità culturale. Si devono considerare eventuali differenze culturali nelle percezioni del rischio: platee con background diversi potrebbero interpretare in modo differente concetti come privacy, fiducia nell'autorità o condivisione di informazioni. Un approccio inclusivo adegua la comunicazione tenendo conto di tali differenze, per incontrare il pubblico nel proprio contesto. Questo può voler dire usare metafore ed esempi

[6] ENISA – European Union Agency for Cybersecurity, *Awareness and Cyber Hygiene*, 2023, https://www.enisa.europa.eu/.

[7] ENISA – European Union Agency for Cybersecurity, *Awareness and Cyber Hygiene*, 2023, https://www.enisa.europa.eu/.

comprensibili e rilevanti in una data cultura, evitare riferimenti culturali non familiari, e magari coinvolgere ambasciatori locali che rendano il messaggio più credibile. In ambito europeo esistono linee guida per localizzare efficacemente le campagne di sicurezza informatica, così da coprire l'intero spettro dei cittadini UE [8]. Il risultato cercato è una cultura cyber diffusa e condivisa, che tenga conto delle pluralità linguistiche e culturali ma affermi princìpi comuni di igiene informatica.

2.4. Apprendimento permanente e adattivo (lifelong learning)

Le conoscenze e minacce informatiche evolvono rapidamente, rendendo indispensabile un *apprendimento continuo* lungo tutto l'arco della vita professionale, e non, degli individui. Un singolo corso una tantum non basta: le competenze cyber devono essere costantemente aggiornate tramite programmi di formazione continua [9]. Un approccio inclusivo prevede quindi *percorsi di lifelong learning*, accessibili in modo flessibile (e-learning, webinar periodici, pillole formative) affinché ognuno possa apprendere nei propri tempi e secondo necessità emergenti. Ad esempio, un impiegato potrebbe seguire ogni anno moduli di aggiornamento sulle nuove tipologie di phishing o sulle politiche aziendali riviste, mentre un pensionato che si affaccia all'home banking dovrebbe avere a disposizione risorse formative elementari ma aggiornate per navigare in sicurezza. Le istituzioni e le aziende iniziano a promuovere piattaforme di apprendimento permanente sulla cybersicurezza: in Italia l'ACN stessa sottolinea l'importanza di "irrobustire la sicurezza digitale investendo sulla formazione delle competenze umane", poiché personale non preparato può trasformare la propria incompetenza in un errore fatale [10]. L'educazione adattiva, supportata da algoritmi che suggeriscono contenuti in base al profilo dell'utente, può aiutare a mantenere alto l'ingaggio nel tempo. In definitiva, la manutenzione delle competenze di cybersecurity deve diventare parte integrante del percorso lavorativo e formativo di ognuno, analogamente a quanto avviene per le competenze tecniche: solo così si garantisce che la difesa dai rischi informatici resti efficace di fronte a minacce nuove e scenari in mutamento.

---

[8] ENISA – European Union Agency for Cybersecurity, *Awareness and Cyber Hygiene*, 2023, https://www.enisa.europa.eu/.

[9] Agenzia per la Cybersicurezza Nazionale (ACN), *Strategia Nazionale di Cybersicurezza 2022-2026*, 2022.

[10] Agenzia per la Cybersicurezza Nazionale (ACN), *Strategia Nazionale di Cybersicurezza 2022-2026*, 2022.

3. Iniziative e policy sulla dimensione umana della cybersicurezza

Sia a livello nazionale che internazionale, cresce l'attenzione verso politiche e programmi che riconoscono la centralità del fattore umano nella cybersicurezza. Oltre agli interventi puramente tecnologici, strategie governative e normative recenti enfatizzano la formazione, la sensibilizzazione e lo sviluppo di competenze come pilastri della sicurezza collettiva. Di seguito alcune delle principali iniziative in tal senso, inquadrando prima il contesto italiano e poi quello europeo [11].

3.1. Strategia nazionale di cybersicurezza e cultura della sicurezza

L'Italia si è dotata di una *Strategia Nazionale per la Cybersicurezza 2022-2026*, che include esplicitamente misure volte a rafforzare il fattore umano. All'interno vi è una sezione dedicata alla "*Promozione della cultura della sicurezza cibernetica*", riconoscendo che solo tramite una maggiore consapevolezza diffusa è possibile ridurre la superficie d'attacco [12]. Nel 2024 è stata lanciata la campagna istituzionale "*Accendiamo la cybersicurezza. Proteggiamo le nostre imprese*", promossa *dall'Agenzia per la Cybersicurezza Nazionale (ACN)* insieme alla Presidenza del Consiglio, proprio con l'obiettivo di rafforzare il fattore umano nella difesa delle PMI [13]. La campagna mira ad accelerare la presa di coscienza del ruolo chiave della cybersecurity nella transizione digitale del Paese e a fornire a cittadini e imprese informazioni essenziali per tutelare la propria vita economica e sociale [14]. In generale, la strategia nazionale prevede molteplici azioni coordinate, molte delle quali coinvolgono aspetti umani: dalla formazione di figure specializzate alla sensibilizzazione nelle scuole e tra i cittadini.

[11] Per approfondimenti sull'evoluzione normativa e le strategie di governo, si rimanda ai contributi della Parte I di questo Volume.

[12] ACN & Dipartimento per l'Informazione e l'Editoria, *Accendiamo la cybersicurezza. Proteggiamo le nostre imprese. Campagna di sensibilizzazione*, 2024.

[13] ACN & Dipartimento per l'Informazione e l'Editoria, *Accendiamo la cybersicurezza. Proteggiamo le nostre imprese. Campagna di sensibilizzazione*, 2024.

[14] ACN & Dipartimento per l'Informazione e l'Editoria, *Accendiamo la cybersicurezza. Proteggiamo le nostre imprese. Campagna di sensibilizzazione*, 2024.

3.2. Ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) e programmi educativi

L'ACN ha tra i suoi mandati la promozione di una cultura della sicurezza e lo sviluppo di competenze cyber nel tessuto socio-economico. Sul fronte educativo, promuove la formazione continua sulla cybersicurezza collaborando con il Ministero dell'Istruzione e offrendo corsi tramite Scuola Futura per docenti, creando percorsi ITS per la sicurezza informatica e coordinandosi con università (laboratori, dottorati PNRR come SERICS). ACN realizza campagne di sensibilizzazione rivolte a PMI, giovani talenti, sostenendo le olimpiadi della cybersecurity e la *European Cybersecurity Challenge 2024*, e Pubblica Amministrazione. Ha prodotto un glossario online, risorse come webinar e moduli e-learning. L'Agenzia rafforza inoltre la collaborazione pubblico-privato e il coinvolgimento dei cittadini nella "civil alliance" per la cybersecurity, riconoscendo il ruolo centrale del fattore umano. In sintesi, ACN è un catalizzatore nazionale per iniziative che integrano aspetti normativi, formativi e comunicativi.

3.3. Quadro normativo europeo e programmi di sensibilizzazione

Anche a livello europeo, la dimensione umana è parte integrante delle politiche di cybersicurezza. La nuova *Direttiva NIS2 (UE 2022/2555)* – recepita in Italia con d.lgs. n. 138/2024 – impone esplicitamente obblighi di formazione e sensibilizzazione: gli enti essenziali dovranno erogare training periodici in materia di sicurezza informatica sia al personale operativo sia al management [15]. In parallelo, il *Regolamento Generale sulla Protezione dei Dati (GDPR)* richiede alle organizzazioni di formare i propri dipendenti sulle misure di sicurezza e privacy. Entrambi convergono dunque nel riconoscere la formazione del personale come prerequisito fondamentale per raggiungere un'adeguata resilienza e una reale protezione dei dati [16]. Questa enfasi regolatoria ha lo scopo di radicare una diffusa *cultura della sicurezza* nei settori pubblico e privato: solo attraverso una sensibilizzazione capillare "a tutti i livelli" si può ottenere il cambiamento culturale necessario a ridurre i rischi cyber [17].

Sul fronte operativo, l'Unione Europea sostiene numerosi programmi dedicati alle competenze e alla consapevolezza. L'ENISA (Agenzia UE per la cybersicurezza) coordina dal 2012 il *Mese Europeo della Cybersecurity (ECSM)* ogni ottobre, una campagna annuale in tutti i Paesi membri con eventi, materiali

[15] AGENDA DIGITALE, *NIS2: nuove responsabilità per aziende e PA*, 2023.

[16] AGENDA DIGITALE, *NIS2: nuove responsabilità per aziende e PA*, 2023.

[17] AGENDA DIGITALE, *NIS2: nuove responsabilità per aziende e PA*, 2023.

informativi e contenuti social rivolti ai cittadini e alle imprese. ENISA, con il supporto della Commissione, ha pubblicato guide pratiche per le campagne nazionali di *awareness* e promuove lo scambio di best practice tra Stati membri [18]. In un'ottica di cyber hygiene generale, l'agenzia punta a fomentare cambiamenti comportamentali e consolidare un ecosistema "diverso, resiliente e consapevole" in cui le buone abitudini di sicurezza diventino standard in tutti i settori [19]. Un'iniziativa recente di rilievo è la *Cybersecurity Skills Academy*, lanciata dalla Commissione Europea nel 2023, che mira a colmare la carenza di competenze cyber attraverso un approccio comune alla formazione e a piattaforme di e-learning aperte a studenti, lavoratori e cittadini in cerca di riqualificazione. Contestualmente, la *Digital Skills and Jobs Coalition* europea include la cybersicurezza tra le competenze digitali chiave da diffondere, con impegni congiunti di governi e aziende per formare milioni di europei sulle competenze di base di sicurezza ICT. Si può citare anche l'*European Cybersecurity Organisation (ECSO)* che con il suo gruppo di lavoro *Skills & Human Factors* contribuisce allo sviluppo di framework europei per le competenze cyber e incoraggia la partecipazione di gruppi sotto-rappresentati alla forza lavoro cyber [20]. In sostanza, a livello UE si sta costruendo un ecosistema di politiche, fondi e strumenti che affrontano la cybersicurezza non solo come questione tecnica ma come sfida socio-educativa, in linea con il principio che "*la sicurezza informatica è una responsabilità condivisa*" di tutti i cittadini e organizzazioni.

4. Case study ed esempi di formazione inclusiva

Per concretizzare i princìpi precedentemente esposti, è utile esaminare alcuni casi reali di iniziative volte a coinvolgere attivamente e in modo inclusivo diversi contesti: dal pubblico generale, al mondo aziendale, fino alla scuola.

4.1. Campagne pubbliche di sensibilizzazione (settore pubblico e PMI)

Uno degli esempi più rilevanti è la già menzionata campagna "*Accendiamo la cybersicurezza. Proteggiamo le nostre imprese*" rivolta alle PMI italiane.

---

[18] ENISA – European Union Agency for Cybersecurity, *Awareness and Cyber Hygiene*, 2023, https://www.enisa.europa.eu/.

[19] ENISA – European Union Agency for Cybersecurity, *Awareness and Cyber Hygiene*, 2023, https://www.enisa.europa.eu/.

[20] ECSO – European Cybersecurity Organisation, *Skills and Human Factors Working Group*, 2022.

Questa iniziativa pubblica, lanciata nel 2024 da ACN col Dipartimento Informazione e Editoria, ha utilizzato spot TV, radio, stampa e social media per diffondere consigli pratici di sicurezza informatica a un vasto pubblico di imprenditori, professionisti e dipendenti di piccole aziende [21]. La campagna è stata costruita con un linguaggio semplice e messaggi chiave immediati, proprio per raggiungere anche chi non ha competenze tecniche. Inoltre, ha adottato un approccio multi-target: materiali differenziati per i decisori aziendali (sottolineando l'impatto economico degli attacchi e l'importanza di investire in sicurezza) e per i dipendenti (focalizzando i comportamenti quotidiani corretti). Questo approccio inclusivo assicura che tutti i livelli dell'organizzazione, dal dirigente all'impiegato, siano coinvolti nella crescita della cultura cyber [22]. La scelta di canali tradizionali come TV e radio, oltre al web, è dovuta alla volontà di non escludere le generazioni meno giovani o meno avvezze ai social network. I risultati attesi, e monitorati, riguardano un aumento significativo della consapevolezza: già solo portare l'argomento "cybersecurity" all'attenzione del 99% del tessuto produttivo (le PMI) è un passo avanti in un Paese dove il tema era spesso trascurato. Questa campagna può essere vista come *best practice* di collaborazione istituzionale per rafforzare il fattore umano: ha infatti attuato una misura strategica nazionale e gettato le basi per un'"alleanza" tra governo, imprese e cittadini nella difesa cibernetica.

Un secondo case study interessante proviene dall'ambito comunitario locale: alcune amministrazioni comunali in Italia hanno avviato programmi di formazione per i propri cittadini, spesso in collaborazione con associazioni e università. Ad esempio, sono stati organizzati cicli di incontri pubblici sulla sicurezza online presso biblioteche civiche, con esperti che spiegavano come proteggere i dati personali o usare l'home banking in sicurezza. Questi incontri gratuiti, aperti a tutte le età, rappresentano modalità inclusive di coinvolgere anche segmenti di popolazione a rischio esclusione (anziani, persone con bassa alfabetizzazione digitale). In parallelo, iniziative come la Coalizione "Repubblica Digitale", promossa dal MID, includono progetti dedicati alla sicurezza informatica tra le competenze digitali di base da diffondere: un esempio è il percorso "*Cybersecurity for All*" che alcune associazioni di volontariato digitale stanno portando nelle piccole comunità per insegnare concetti chiave di difesa personale online. Tali iniziative, pur di scala limitata, forniscono modelli replicabili di formazione di prossimità, adattabili alle esigenze locali e quindi altamente inclusivi.

---

[21] ACN & Dipartimento per l'Informazione e l'Editoria, *Accendiamo la cybersicurezza. Proteggiamo le nostre imprese. Campagna di sensibilizzazione*, 2024.

[22] ACN & Dipartimento per l'Informazione e l'Editoria, *Accendiamo la cybersicurezza. Proteggiamo le nostre imprese. Campagna di sensibilizzazione*, 2024.

4.2. Programmi aziendali di sensibilizzazione e formazione continua (contesto corporate)

Nel contesto attuale, caratterizzato da una crescente esposizione alle minacce informatiche, il settore privato sta progressivamente riconoscendo il ruolo cruciale della formazione continua in materia di cybersecurity. In tal senso, la promozione di una "cultura della sicurezza" rappresenta oggi un obiettivo strategico condiviso, in particolare nei settori ad alta criticità operativa. Un esempio emblematico è rappresentato da alcune grandi realtà imprenditoriali italiane che hanno avviato un programma sistemico di formazione e sensibilizzazione alla cybersecurity, in collaborazione con centri di ricerca nazionali. Tra queste, spiccano iniziative come quella promossa dall'Agenzia per la Cybersicurezza Nazionale (ACN) insieme all'Università Bocconi [23], i programmi portati avanti da Cefriel, centro di innovazione digitale del Politecnico di Milano [24], e le attività di BV Tech, che ha attivato percorsi formativi in collaborazione con vari atenei italiani [25]. I vari piani hanno coinvolto un gran numero di dipendenti in una campagna continuativa di formazione alla cybersecurity, con risultati tangibili: è stata registrata una forte riduzione dei comportamenti a rischio dopo il primo ciclo formativo, misurata attraverso audit interni ed esterni. Il modello adottato si fonda su una combinazione di strumenti didattici digitali e tecniche di coinvolgimento attivo. Il programma include sessioni mensili in modalità e-learning con contenuti interattivi e aggiornati, simulazioni periodiche di attacchi informatici, in particolare campagne di phishing simulate, e pratiche di gamification interna. Quest'ultima ha previsto la creazione di classifiche tra reparti basate sulla percentuale di clic su messaggi sospetti o sulla rapidità di segnalazione di incidenti, incentivando una sana competizione orientata alla sicurezza.

Uno degli elementi di forza del modello è la sua struttura modulare e personalizzata per ruolo. I nuovi assunti partecipano a sessioni focalizzate sulla sicurezza di base, mentre i manager sono coinvolti in workshop orientati alla gestione dei rischi strategici e delle crisi cyber. I team tecnici ricevono invece una formazione specialistica continua, allineata alle più recenti evoluzioni delle minacce informatiche.

Questa articolazione formativa consente di diffondere in modo capillare le buone pratiche di sicurezza, adattandole al livello di responsabilità e di esposizione al rischio di ciascun dipendente. L'approccio è coerente con le linee guida

---

[23] AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN), *ACN e Università Bocconi: insieme per rafforzare la cultura della cybersecurity*, 2024.

[24] CEFRIEL – POLITECNICO DI MILANO, *Innovazione digitale e sicurezza informatica: il ruolo della formazione*, Cefriel, 2024.

[25] B.V. TECH, *Formazione e sviluppo di competenze in ambito cybersecurity*, 2024.

promosse da standard internazionali come la ISO/IEC 27001, che enfatizzano l'importanza della sensibilizzazione e della formazione continua come parte integrante del sistema di gestione della sicurezza delle informazioni.

Particolarmente innovativo risulta l'inserimento di tecniche esperienziali nei programmi formativi, come le *escape room* a tema cyber. Queste attività coinvolgono piccoli gruppi di dipendenti in simulazioni di scenari critici, come la gestione di un attacco simulato, stimolando la collaborazione, la risoluzione di problemi e la comprensione concreta delle conseguenze operative di un incidente informatico. L'impiego di queste tecniche, sperimentate anche in contesti istituzionali a livello europeo, ha dimostrato di aumentare significativamente l'engagement dei partecipanti e la loro capacità di trasferire le conoscenze acquisite nel contesto lavorativo reale.

Nel complesso, l'evidenza empirica raccolta in diversi casi aziendali suggerisce che un approccio integrato fondato su formazione continuativa, simulazioni pratiche, coinvolgimento attivo dei dipendenti e supporto diretto del top management, sia particolarmente efficace nel rafforzare la postura di sicurezza delle organizzazioni. La diffusione di una cultura della sicurezza condivisa e interiorizzata contribuisce a ridurre il peso degli errori umani nei processi critici e a rendere l'intera organizzazione più resiliente di fronte agli attacchi informatici.

4.3. Formazione nelle scuole e contesti educativi

Anche il mondo dell'istruzione sta riconoscendo l'importanza di includere la cybersecurity nei percorsi formativi, adottando modalità inclusive per preparare sia i giovani sia il personale docente. Sul fronte dei curricula scolastici, il Ministero ha introdotto nell'ambito dell'Educazione Civica digitale temi legati alla sicurezza online (es. tutela della privacy, contrasto al cyberbullismo, uso sicuro dei social media). Molte scuole secondarie si stanno attivando per fornire *laboratori di coding e sicurezza*, spesso con il supporto di esperti esterni oppure tramite una formazione con un modello di *peer education*: studenti delle classi superiori, formati tramite workshop di base sulla cybersecurity, diventano tutor per gli allievi più giovani, insegnando loro in modo informale come proteggere i propri account o riconoscere le truffe online. Questo metodo favorisce l'inclusione perché utilizza il linguaggio dei ragazzi e crea un ambiente di apprendimento paritario.

La formazione dei docenti è un tassello cruciale: attraverso piattaforme come *Scuola Futura*, finanziata dal PNRR, migliaia di insegnanti di ogni ordine e grado stanno seguendo corsi di aggiornamento su competenze digitali e sicurezza di base, imparando sia a proteggere le proprie classi sia a trasmettere queste

conoscenze agli studenti [26]. Dotare i docenti degli strumenti per insegnare la cybersicurezza in maniera inclusiva significa garantire un effetto moltiplicatore: raggiungere tutti gli studenti, compresi quelli con difficoltà, e formare una nuova generazione più consapevole e preparata di cittadini digitali.

5. Formazione giovanile e consapevolezza digitale: un presidio contro le minacce informatiche

La digitalizzazione ha trasformato in maniera profonda il mondo dell'istruzione, del lavoro e della vita quotidiana. In questo contesto, la formazione digitale rivolta ai giovani non rappresenta solo un investimento in termini di competenze professionali, ma una misura preventiva cruciale contro le nuove forme di rischio connesse all'uso della tecnologia. La crescente esposizione a minacce informatiche come phishing, violazioni della privacy, furti d'identità e manipolazioni dell'informazione richiede un'alfabetizzazione digitale solida e consapevole, che deve iniziare già nei primi gradi scolastici.

La sicurezza informatica, in particolare, assume un ruolo sempre più rilevante come dimensione trasversale nei processi educativi. L'apprendimento delle competenze digitali di base non può prescindere da una riflessione critica sull'uso consapevole della rete, sui comportamenti da adottare per tutelare i propri dati e sull'importanza di riconoscere potenziali minacce digitali. Il documento in oggetto sottolinea la necessità di percorsi formativi mirati, sviluppati lungo l'intero ciclo scolastico e adattati alle diverse fasce d'età, con l'obiettivo di costruire una cittadinanza digitale attiva, inclusiva e resiliente.

5.1. Progetti educativi per la consapevolezza informatica

Tra alcune delle iniziative più significative nell'ambito della formazione giovanile vi è il progetto "Ragazze Digitali", che affronta in modo diretto la questione della sotto-rappresentazione femminile nel settore tecnologico. Il progetto nasce dalla consapevolezza che molti ostacoli alla partecipazione delle donne nel mondo ICT derivano da stereotipi sociali, da un'errata percezione dell'informatica e da una carenza di esperienze dirette che mostrino il carattere creativo e applicativo della disciplina. Nei *summer camp* della Romagna, le ragazze partecipanti affrontano un percorso completo che le introduce alla progettazione di applicazioni mobili, partendo dallo sviluppo dell'interfaccia grafica, passando

[26] MINISTERO DELL'ISTRUZIONE E DEL MERITO, *Piattaforma Scuola Futura: formazione su competenze digitali e sicurezza*, 2023.

per la logica applicativa, fino all'uso di API e strumenti di intelligenza artificiale. Particolarmente significativo è il fatto che le partecipanti, spesso al loro primo contatto con il mondo dell'informatica, riescono a realizzare prototipi funzionanti, aumentando la loro autostima, il senso di autoefficacia e la capacità di lavorare in gruppo. Durante la seconda parte del camp viene introdotto un modulo di formazione sull'intelligenza artificiale, con attenzione anche agli aspetti legati alla sicurezza e all'etica. Le ragazze sviluppano in team un'applicazione su un tema a loro scelta, che viene presentata pubblicamente a fine percorso. Questa esperienza permette non solo di apprendere competenze tecniche, ma anche di comprendere la rilevanza della sicurezza informatica e del comportamento responsabile online, contribuendo a formare giovani utenti consapevoli e potenzialmente futuri professionisti della cybersicurezza. Il progetto è stato riconosciuto anche a livello europeo come caso virtuoso: il report *She Figures 2021* [27] menziona Ragazze Digitali come l'unico esempio italiano di iniziativa strutturata per promuovere la partecipazione femminile nel settore ICT attraverso percorsi formativi innovativi rivolti alle giovani studentesse.

5.2. Il ruolo della scuola e dei percorsi PCTO

Un ambito rilevante delle attività legate al progetto SERICS è rappresentato dai Percorsi per le Competenze Trasversali e l'Orientamento (PCTO), realizzati in collaborazione con istituti scolastici secondari. Diverse università partner del progetto hanno attivato laboratori formativi rivolti a studenti e studentesse delle scuole superiori, con un focus sul pensiero computazionale e sul *coding*. Tali attività hanno l'obiettivo di far acquisire ai giovani il pensiero computazionale come quarta abilità di base, al pari della lettura, della scrittura e del calcolo. In particolare, attraverso esercizi pratici, utilizzo di piattaforme di programmazione visuale e lavori di gruppo, gli studenti apprendono non solo come funziona un algoritmo, ma anche come si struttura un ragionamento logico coerente, come si gestisce un progetto informatico e, aspetto centrale, come identificare criticità e vulnerabilità nel funzionamento di un sistema.

Questi percorsi rafforzano nei giovani la capacità di risolvere problemi, collaborare in modo efficace e riflettere sugli impatti sociali e comportamentali della tecnologia. Anche in questo caso, l'approccio formativo si basa su attività collaborative e orientate al progetto, che stimolano lo sviluppo di competenze pratiche e favoriscono una comprensione diretta delle potenzialità e dei rischi degli strumenti digitali.

---

[27] EUROPEAN COMMISSION, *She Figures 2021 – Gender in research and innovation – Statistics and indicators*, Publications Office of the European Union, 2021.

5.3. Cybersecurity come strumento educativo

L'introduzione della cybersicurezza nei percorsi educativi è centrale per rispondere alla trasformazione digitale in atto. I progetti descritti nel documento dimostrano come un'educazione alla sicurezza non debba limitarsi a regole tecniche o normative, ma possa diventare parte integrante di una visione ampia dell'autonomia digitale. Nei percorsi descritti, i giovani imparano a riconoscere forme comuni di minaccia digitale, come il phishing, l'accesso non autorizzato ai dati, l'uso improprio delle credenziali o il download inconsapevole di software malevoli, rafforzando così le buone pratiche per la tutela della privacy, la gestione sicura delle password, l'uso consapevole dei social media.

L'effetto educativo di questi progetti ha una portata generazionale: i giovani coinvolti diventano non solo utenti più sicuri, ma anche "*ambasciatori digitali*" nei loro contesti familiari e sociali, diffondendo consapevolezza e responsabilità tra i coetanei e gli adulti. Questo approccio, che unisce formazione tecnica ed empowerment, contribuisce a costruire un ecosistema digitale più sicuro, inclusivo e cooperativo.

5.4. Implicazioni strutturali e politiche

La formazione digitale dei giovani dovrebbe costituire un elemento centrale nelle politiche pubbliche orientate all'innovazione e all'inclusione sociale. Il Piano Nazionale di Ripresa e Resilienza (PNRR), in sinergia con il d.m. n. 65/ 2023, promuove interventi specifici per il potenziamento delle competenze STEM, con particolare attenzione alla partecipazione delle studentesse, all'integrazione delle tecnologie nei percorsi curricolari e al superamento del divario digitale di genere. Le azioni previste includono iniziative educative fin dalla scuola primaria, proseguendo con percorsi strutturati nella scuola secondaria e programmi formativi in ambito universitario. Questi interventi non solo favoriscono l'acquisizione di competenze digitali, ma contribuiscono anche a rafforzare la sicurezza informatica dell'intero sistema educativo, formando nuove generazioni consapevoli, responsabili e orientate all'etica digitale e alla collaborazione.

6. Competenze digitali, etica e comportamenti a rischio

In chiusura, è importante riflettere su come il fattore umano in cybersicurezza si leghi a questioni di competenze digitali di base, etica nell'uso della tecnologia e abitudini comportamentali. Molte vulnerabilità, infatti, derivano

non da falle tecniche avanzate, ma da *comportamenti a rischio* dettati da scarsa competenza o superficialità. Come evidenziato, ancora oggi tanti utenti "*non sono abbastanza consapevoli dei fondamenti della sicurezza informatica neanche per un uso quotidiano degli strumenti*". Ad esempio, pratiche rischiose diffuse includono: riutilizzare la stessa password su molti servizi, cliccare link o allegati senza verificarne la fonte, installare app pirata o non aggiornare i software, condividere troppe informazioni personali sui social. Colmare queste lacune rientra nel più ampio obiettivo di sviluppare le competenze digitali della popolazione: nei framework europei, la *sicurezza* è uno dei pilastri della competenza digitale, insieme a capacità di uso critico e consapevole della tecnologia. Questo significa che un utente digitalmente competente non sa solo utilizzare strumenti, ma comprende anche i rischi associati e adotta misure di protezione di base. Investire sul fattore umano in cybersecurity quindi si sovrappone con gli sforzi di *alfabetizzazione digitale* generale, due aspetti che dovrebbero procedere di pari passo.

Un altro aspetto da integrare nei programmi formativi è l'etica digitale. La cybersecurity non riguarda solo il proteggersi dai criminali, ma anche l'usare la tecnologia in modo responsabile e conforme a princìpi etici. In un'era di fake news, sorveglianza digitale e intelligenza artificiale, è fondamentale educare gli utenti a valori come la privacy, il rispetto della proprietà intellettuale, la netiquette nelle comunicazioni online e la responsabilità individuale nel segnalare vulnerabilità o incidenti (responsible disclosure). Ad esempio, un dipendente che scopra una debolezza nel sistema informativo dovrebbe sentirsi eticamente tenuto a segnalarla invece di ignorarla; uno studente hacker alle prime armi va guidato a canalizzare le sue abilità in modo etico.

Oggi, l'etica digitale si intreccia in modo sempre più stretto con le questioni sollevate dall'intelligenza artificiale. Le tecnologie di AI, seppur potenti e innovative, possono rafforzare discriminazioni, violare la privacy o manipolare l'opinione pubblica attraverso l'uso improprio di dati e algoritmi. È quindi essenziale che i percorsi educativi, soprattutto quelli destinati ai giovani, includano momenti di riflessione critica sull'uso responsabile dell'AI. Gli studenti devono essere messi in condizione di comprendere non solo come funzionano gli strumenti basati sull'intelligenza artificiale, ma anche quali implicazioni etiche derivano dalle loro scelte progettuali e dal loro utilizzo nella vita quotidiana, nella scuola e nel lavoro.

Diverse iniziative promuovono oggi il concetto di "cyber ethics": alcune università italiane hanno inserito moduli di etica e diritto informatico nei corsi di sicurezza, mentre associazioni come ISACA [28] o Clusit [29] organizzano workshop

[28] ISACA, *Cybersecurity Fundamentals Study Guide*, 2022.

[29] CLUSIT, *Rapporto Clusit sulla Sicurezza ICT in Italia*, 2023.

su temi etici, come l'"ethical hacking" o la responsabilità algoritmica. Anche l'Agenzia per la Cybersicurezza Nazionale, nei suoi interventi pubblici, richiama spesso la necessità di "un'alleanza civile" che implichi comportamenti etici condivisi e il rispetto delle regole nel cyberspazio [30]. In questo contesto, è fondamentale coltivare nei giovani non solo le competenze tecniche, ma anche una solida coscienza etica, capace di guidarli nel progettare, utilizzare e valutare soluzioni digitali e sistemi intelligenti in modo equo, trasparente e responsabile.

Infine, affrontare i comportamenti a rischio significa lavorare sul cambio di mentalità degli utenti. La sicurezza informatica dovrebbe entrare nella routine quotidiana come lo è allacciarsi la cintura in auto: un gesto naturale e quasi automatico. Per arrivare a ciò, gli esperti raccomandano di puntare molto sulla pedagogia digitale e le buone pratiche: dall'infanzia (insegnando ai bambini concetti semplici come non fidarsi degli sconosciuti online, in parallelo al mondo offline) fino alla formazione continua per adulti (esercitazioni periodiche per rinsaldare le abitudini corrette). Nel già citato articolo "Il fattore umano e la regolazione della cybersecurity", si conclude proprio invitando a adottare un approccio che favorisca "*maggiore pedagogia digitale*" e diffonda buone pratiche nel cyberspazio [31]. Ciò comprende anche l'incoraggiare un atteggiamento proattivo, senza timore di figurare incompetenti, anzi premiando chi contribuisce alla sicurezza collettiva. Allo stesso modo, sul piano individuale, "*da un grande potere derivano grandi responsabilità*": ogni utente dotato di strumenti digitali ha il potere di causare danni, pensiamo a condividere un malware in rete involontariamente, ma anche la responsabilità di comportarsi con prudenza e aiutare gli altri a fare lo stesso.

In conclusione, l'integrazione della dimensione umana nella cybersicurezza, attraverso educazione inclusiva, politiche mirate e sviluppo di competenze ed etica, è la chiave per costruire un ecosistema digitale più sicuro e resiliente. Solo facendo in modo che ogni persona compia la propria parte, consapevole dei rischi e armata degli strumenti conoscitivi giusti, si potrà affrontare efficacemente la complessità delle minacce cibernetiche odierne [32]. La sfida è tanto tecnologica quanto umana: vincerla significa creare una cultura collettiva dove sicurezza, consapevolezza e responsabilità procedano di pari passo.

---

[30] AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN), *Strategia Nazionale di Cybersicurezza 2022-2026*, 2022.

[31] AICA MONDO DIGITALE, *Il fattore umano e la regolazione della cybersecurity*, 2022.

[32] AGENDA DIGITALE, *NIS2: nuove responsabilità per aziende e PA*, 2023.

Capitolo 15

Per un uso consapevole e sicuro delle tecnologie: strategie educative e strumenti di intervento [*]

Valeria Barone [**], Thomas Casadei [***]

Abstract: Il contributo analizza in prospettiva critica l'uso precoce e pervasivo delle tecnologie digitali da parte delle persone minore età, mettendo a fuoco l'ambivalenza tra opportunità e rischi. A partire da dati recenti (UNICEF, OECD, Save the Children, WeProtect) si mostra come l'ecosistema delle piattaforme amplifichi vulnerabilità preesistenti e generi rischi inediti, anche attraverso i cosiddetti "rischi riflessi" prodotti dagli adulti (*sharenting*, *baby influencer*, sollecitando un ripensamento della responsabilità genitoriale, educativa e istituzionale. Su questo tipo di problematiche si sono soffermate le ricerche e le attività del progetto SAFELY – Social media Awareness For Education and Legal Youth che hanno consentito di mettere a punto una serie di strumenti operativi: la mappa dei comportamenti dannosi online, una guida divulgativa multimediale *Giovani in rete* (con podcast, video e interviste). Vengono così delineate alcune strategie per una responsabilità condivisa: dall'alfabetizzazione alla piena cittadinanza digitale; una serie di buone pratiche per famiglie, scuola, mondi formativi; la pratica del dialogo intergenerazionale; il rafforzamento delle competenze di docenti e genitori; la prevenzione integrata e la valorizzazione delle opportunità offerte dalle nuove tecnologie, se utilizzate in modo sicuro e consapevole. In chiusura, si delineano i tratti fondanti dello Sportello informativo SAFELY, un baricentro

---

[*] Il testo è frutto di un percorso comune e di un'elaborazione condivisa, tuttavia, dovendo procedere ad un'attribuzione dei paragrafi, il primo, il quinto e il sesto possono essere attribuiti a Thomas Casadei, il secondo, il terzo e il quarto a Valeria Barone. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

[**] Valeria Barone è Dottoranda di ricerca in "Lavoro, Sviluppo e Innovazione" presso la Fondazione Marco Biagi e l'Univ. di Modena e Reggio Emilia. Fa parte dell'Officina informatica "Diritto Etica e Tecnologie" istituita presso il CRID – Centro di Ricerca su Discriminazione e vulnerabilità, Unimore (www.crid.unimore.it), ed è consulente per il progetto SAFELY (www.safely.unimore.it), valeria.barone@unimore.it.

[***] Thomas Casadei, Ordinario di Filosofia del diritto presso il Dipartimento di Giurisprudenza, è Direttore del CRID – Centro di Ricerca su Discriminazione e vulnerabilità, Unimore, nonché PI del progetto SAFELY. Fa parte, inoltre, della Giunta del CRIS – Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi fondato nel 2007 dal Prof. Michele Colajanni e ora diretto dal Prof. Mirco Marchetti; thomas.casadei@unimore.it.

stabile di supporto e orientamento per studenti, famiglie e insegnanti, nonché una piattaforma per future evoluzioni verso una "clinica legale digitale", capace di connettere ricerca, formazione e tutela effettiva dei diritti delle persone di minore età e dei giovani in generale, nello spazio "onlife".

Keywords: Persone di minore età e tecnologie; cittadinanza digitale; educazione digitale; responsabilità genitoriale e scolastica; mappa dei comportamenti dannosi online; prevenzione e comunità educante; ruolo delle istituzioni.

1. Giovani e tecnologie digitali

1.1. Connettività permanente

L'ingresso delle persone minore età nello spazio digitale avviene oggi in età sempre più precoce. Se fino a pochi anni fa il primo contatto con la rete coincideva con la scuola secondaria, le indagini più recenti [1] mostrano come già nei

[1] UNICEF, *The State of the World's Children 2023: For Every Child, Digital*, New York, 2023; OECD, *Students, Computers and Learning: Making the Connection*, Paris, OECD Publishing, 2023; SAVE THE CHILDREN, *Switched On. Exploring the Impact of Digital Technology on Children's Lives, London*, 2022; D. SMAHEL *et al*., *EU Kids Online 2020: Survey results from*

primi anni della scuola primaria – e talvolta persino nella fascia prescolare – i bambini e le bambine abbiano accesso a dispositivi connessi.

L'ambiente domestico costituisce il primo scenario di "socializzazione tecnologica": smartphone e tablet sono ormai presenze ordinarie nella quotidianità familiare, strumenti che accompagnano i minori nelle attività ludiche, comunicative e, progressivamente, educative [2].

Secondo l'ultimo rapporto dell'OECD *How's Life for Children in the Digital Age* (2025) [3], il 96% dei quindicenni nei paesi OCSE dichiara di avere accesso a un computer desktop, portatile o tablet a casa, mentre il 98% aveva uno smartphone con connessione Internet.

L'aumento della disponibilità di dispositivi ha determinato un corrispondente incremento del tempo trascorso online. Circa un terzo degli adolescenti tra gli 11 e i 15 anni dichiara di essere "quasi costantemente" connesso con amici e conoscenti nel corso della giornata.

Tale connettività permanente [4], da un lato, alimenta forme di socialità immediata e riduce le distanze relazionali; dall'altro, espone le persone di minore età e i giovani, più in generale, a dinamiche di pressione sociale, alla difficoltà di disconnessione e a nuove forme di dipendenza.

Il rapporto *Childhood in a Digital World* di UNICEF [5] invita, tuttavia, a superare approcci semplicistici: non è tanto la quantità di tempo trascorsa online a determinare gli effetti sul benessere psicosociale, quanto piuttosto la qualità delle interazioni e dei contenuti fruiti. L'esposizione a fenomeni come cyberbullismo, *grooming*, contenuti violenti o sessualmente espliciti [6] è strettamente

---

19 countries, EU Kids Online, London School of Economics and Political Science, London, 2020.

[2] Su questi profili si può vedere, S. GARASSINI (a cura di), *Clicco quindi educo: genitori e figli nell'era dei social network*, ETS, Pisa, 2018; P. FERRI, *Figli digitali*, Rizzoli, Milano, 2024. Cfr., anche, G. RIVA, *Io, noi, loro. Le relazioni nell'era dei social e dell'IA*, il Mulino, Bologna, 2025.

[3] https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b90Z0-en.html.

[4] M. GUI (a cura di), *Benessere Digitale a scuola e a casa. Un percorso di educazione ai media nella connessione permanente*, Mondadori, Milano, 2019; *Le sfide educative e sociali della connessione permanente*, intervista al Prof. Marco Gui, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025, pp. 197-206.

[5] UNICEF INNOCENTI – GLOBAL OFFICE OF RESEARCH AND FORESIGHT, *Childhood in a Digital World*, Florence, 2025.

[6] Per un approfondimento volto a chiarire quali condotte possano essere qualificate come comportamenti dannosi online – e, al contempo, per comprendere quali pratiche sia opportuno evitare – si rinvia alla "Mappa alfabetica dei comportamenti dannosi online", disponibile sul portale del progetto SAFELY (https://www.safely.unimore.it).

correlata a un aumento dei livelli di ansia e depressione, così come a condotte autolesive. Al contrario, l'uso creativo, educativo e partecipativo delle tecnologie può favorire lo sviluppo cognitivo, l'inclusione sociale e l'autonomia.

Accanto a queste dinamiche, cresce il fenomeno delle interazioni online con persone sconosciute. Il rapporto di Save the Children e Western Sydney University (2023) [7] mostra che circa due terzi dei minori connessi interagiscono quotidianamente con individui mai incontrati prima, nonostante la consapevolezza dei rischi di adescamento. Parallelamente, il *Global Threat Assessment* di WeProtect (2023) registra un aumento dell'87% nelle segnalazioni di materiale di abuso sessuale su persone di minore età rispetto al 2019, segnalando come la rete costituisca un contesto che strutturalmente determina situazioni di vulnerabilità [8], nel quale i minori rischiano di essere esposti a forme di sfruttamento e di abuso senza precedenti [9].

1.2. Tra rischi e opportunità

L'insieme di questi dati mette in luce una condizione ambivalente. L'accesso precoce al digitale è ormai un dato strutturale delle società contemporanee e non può essere letto unicamente in termini di rischio o, al contrario, di sole opportunità. Esso rappresenta un campo di possibilità nel quale i minori si muovono con naturalezza, ma nel quale mostrano anche tutta la loro fragilità.

La sfida per educatori, famiglie e istituzioni consiste quindi non nell'impedire l'accesso, ma nel governarlo, accompagnando bambini, bambine e adolescenti verso un uso consapevole e critico degli strumenti che ormai costituiscono parte integrante della loro vita quotidiana.

L'accesso alle tecnologie digitali da parte dei minori non si limita a rappresentare una questione di disponibilità di dispositivi o di tempo trascorso online: esso costituisce un'esperienza complessa e ambivalente, capace di generare, al

---

[7] SAVE THE CHILDREN – WESTERN SYDNEY UNIVERSITY, *Our Digital Lives: The Impact of Technology on Children's Wellbeing*, 2023.

[8] Cfr. G. MALGIERI, *Vulnerability and Data Protection Law*, Oxford University Press, Oxford, 2023; S. DADÀ, *Vulnerabilità digitale: etica, intelligenza artificiale e medicina*, Mimesis, Milano-Udine, 2024.

Con particolare riguardo all'AI Act si veda F. GALLI-C. NOVELLI, *The Many Meanings of Vulnerability in the AI Act and the One Missing*, in *BioLaw Journal – Rivista di BioDiritto*, 2024, 1, pp. 53-72.

[9] Si veda, al riguardo, S. PIETROPAOLI, *Informatica criminale Diritto e sicurezza nell'era digitale. Aggiornata alla legge 90/2024 e alla direttiva NIS2*, Giappichelli, Torino, 2025, il quale prende in esame in particolare pedopornografia, adescamento di minori e pornografia virtuale: pp. 32-34.

contempo, opportunità di apprendimento e forme inedite di socialità, ma anche vulnerabilità e rischi difficili da affrontare. Questa ambivalenza è uno dei tratti più evidenti della condizione digitale contemporanea, uno spazio in cui bambini, bambine e adolescenti si muovono agilmente ma senza disporre sempre delle competenze critiche e delle adeguate tutele per orientarsi in contesti tanto ricchi di opportunità quanto densi di insidie.

Dal punto di vista della *dimensione educativa*, le tecnologie offrono un ventaglio straordinario di possibilità. La rete, se accompagnata da un uso consapevole e da un'adeguata mediazione adulta, consente di ampliare l'accesso a contenuti culturali e formativi, di sperimentare modalità di apprendimento personalizzate e interattive, di colmare distanze geografiche e disuguaglianze territoriali. Le iniziative promosse dall'UNESCO e dall'UNICEF [10] hanno più volte sottolineato il ruolo del digitale come fattore di inclusione per i minori che vivono in contesti marginali o privi di risorse educative tradizionali, permettendo loro di accedere a materiali didattici e di partecipare a progetti transnazionali di scambio e cooperazione. In tal senso, l'*alfabetizzazione digitale* si configura come un nuovo diritto di cittadinanza, strettamente connesso all'eguaglianza sostanziale delle opportunità educative [11].

Non meno rilevante è la *dimensione sociale*. L'universo digitale ha trasformato in modo radicale le modalità di costruzione e mantenimento delle relazioni tra pari. Attraverso i social network, le piattaforme di messaggistica e i giochi online, bambini, bambine e adolescenti instaurano legami che rafforzano le amicizie esistenti e, al contempo, aprono lo spazio per comunità transnazionali di interessi condivisi. L'esperienza digitale diventa così uno dei principali luoghi di formazione identitaria e di sperimentazione di ruoli sociali, con un'intensità forse senza precedenti nella storia. Tuttavia, questa connettività permanente presenta un rovescio della medaglia: la pressione a mantenere costantemente aggiornato il proprio profilo, il confronto continuo con i coetanei, la ricerca di approvazione attraverso i like e le visualizzazioni possono alimentare ansia da

---

[10] Tra le principali iniziative globali si ricordano, per l'UNESCO, il programma *Futures of Education*, il progetto congiunto *Gateways to Public Digital Learning* (con UNICEF); nonché strumenti operativi come OpenEMIS, destinati al monitoraggio dei sistemi educativi. Sul versante UNICEF, si segnalano il programma *Keeping Children Safe Online*; l'iniziativa Giga, lanciata con ITU, che mira a connettere tutte le scuole del mondo entro il 2030; e il *Learning Passport*, piattaforma digitale/offline sviluppata con Microsoft per garantire continuità educativa in contesti di crisi o emergenza. (cfr. UNESCO, *Futures of Education. A New Social Contract for Education*, 2021; UNICEF, *Keeping Children Safe Online*, 2023).

[11] Fondamentale in merito è M.N. CAMPAGNOLI-A.C. AMATO MANGIAMELI, *Strategie digitali. #diritto_educazione_tecnologia*, Giappichelli, Torino, 2020. Cfr., inoltre, B.G. BELLO, *(In)Giustizie digitali. Un itinerario su tecnologie e diritti*, Pacini, Pisa, 2023, in part. pp. 112-113.

prestazione, disturbi dell'autostima e un senso di esposizione permanente al giudizio altrui [12].

Sul versante dei rischi, infatti, il digitale non solo amplifica dinamiche già presenti nei contesti offline, ma le proietta in una dimensione caratterizzata da una portata e una velocità che sfuggono ai tradizionali strumenti di controllo. Al tempo stesso, l'ambiente online genera rischi inediti [13], sui quali ci si soffermerà più dettagliatamente nel prossimo paragrafo.

1.3. Una sfida educativa e istituzionale

Alla luce di quanto osservato, per ora basti accennare ad alcuni esempi. Il cyberbullismo rappresenta quello più evidente: le offese e le prevaricazioni che un tempo si esaurivano nello spazio fisico della scuola possono oggi dilagare senza limiti, raggiungendo il minore in ogni momento della sua vita quotidiana.

Altrettanto rilevanti sono i fenomeni di *sexting*, di diffusione non consensuale di immagini intime e di esposizione a contenuti violenti o sessualmente espliciti [14].

A questi si aggiungono le pratiche di disinformazione (il fenomeno delle cosiddette *fake news*) [15], particolarmente insidiose in una fase dello sviluppo in cui il pensiero critico è ancora in formazione, e le forme di dipendenza tecnologica, che si manifestano attraverso l'uso compulsivo dei videogiochi o dei social media.

Un ulteriore elemento da considerare riguarda la riproduzione delle disuguaglianze. I minori provenienti da famiglie con minori risorse culturali ed economiche tendono a utilizzare le tecnologie soprattutto in modo passivo e ricreativo, con scarso accesso a contenuti educativi o ad attività di *empowerment*

---

[12] L. FASSI-A.M. FERGUSON-A.K. PRZYBYLSKI *et al*., *Social media use in adolescents with and without mental health conditions*, in *Nature Human Behaviour*, 2025, vol. 9, n. 6, pp. 1283-1299. Sulla questione dell'ansia si vedano le tesi provocatorie di J. HAIDT, *La generazione ansiosa. Come i social hanno rovinato i nostri figli*, Rizzoli, Milano, 2024.

[13] Tra i rischi inediti si segnalano: la produzione e diffusione di *deepfake* e altre manipolazioni audiovisive, che possono ledere la reputazione e favorire fenomeni di ricatto; le nuove forme di dipendenza (notifiche continue, sistemi di ricompensa, micro-transazioni) che accentuano l'iperconnessione giovanile; la circolazione incontrollata di dati personali connessa alla profilazione algoritmica; l'esposizione precoce a contenuti estremi (violenti, sessualizzati, autolesivi), che incidono sui processi identitari ed emotivi dei minori.

[14] Su questi fenomeni si rinvia a S. PIETROPAOLI, *Informatica criminale Diritto e sicurezza nell'era digitale. Aggiornata alla legge 90/2024 e alla direttiva NIS2*, cit., pp. 30-32.

[15] C. CONIGLIONE, *Falsità delle informazioni e comunicazione in rete: le fake news*, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, cit., pp. 101-112.

digitale. Al contrario, chi cresce in contesti più favoriti beneficia più facilmente di una mediazione adulta attenta e di un impiego del digitale orientato all'apprendimento e alla creatività. In questo senso, il digitale non elimina le disparità preesistenti, ma rischia di accentuarle, configurando un "*digital divide* di seconda generazione", legato non solo alla disponibilità dei dispositivi, ma soprattutto alla qualità e agli scopi dell'uso [16].

La sfida educativa e politico-istituzionale consiste, dunque, nel creare condizioni in cui i minori possano sperimentare i benefici del digitale senza esserne sopraffatti, sviluppando competenze critiche, strumenti di resilienza e reti di protezione efficaci. Solo in questo equilibrio dinamico sarà possibile tradurre il potenziale delle tecnologie in un reale fattore di emancipazione e di autonomia e non in una nuova causa di esclusione o vulnerabilità.

2. Principali minacce

2.1. Dipendenze comportamentali e autoreclusione

L'iperconnessione è divenuta la cifra distintiva della vita quotidiana dei più giovani, al punto da modificare radicalmente le forme di apprendimento, socialità e tempo libero. La distinzione tra uso "funzionale" e uso "ricreativo" delle tecnologie risulta sempre più sfumata, e le giornate degli adolescenti si articolano ormai in un flusso continuo di interazioni mediate da schermi. I dati comparativi raccolti dall'OCSE (2023) confermano questa tendenza: i quindicenni trascorrono in media 2 ore al giorno su dispositivi digitali per attività didattiche a scuola, a cui si sommano 1,5 ore prima o dopo le lezioni e 1,6 ore nel weekend. L'uso per attività di svago è altrettanto significativo: 1,1 ore al giorno a scuola, 2,6 ore prima/dopo e 3,9 ore nel fine settimana. Complessivamente, oltre la metà degli adolescenti utilizza strumenti digitali per più di 30 ore a settimana, con picchi che superano le 60 ore nei casi più intensi (in Italia e Lettonia questa percentuale raggiunge il 43%).

A fronte di questo scenario, le linee guida internazionali sollevano un ulteriore elemento di riflessione. L'Organizzazione Mondiale della Sanità, pur non avendo fissato raccomandazioni precise per gli adolescenti (come invece per i bambini sotto i 5 anni), sottolinea i rischi di un'esposizione prolungata e invita

[16] Si tratta di aspetti particolarmente evidenti se si prendono in esame le condizioni dei cosiddetti "minori stranieri non accompagnati": TH. CASADEI-B. G. BELLO (a cura di), *Minori stranieri non accompagnati ed esercizio dei diritti. Sicurezza, consapevolezza, uso delle tecnologie*, Mucchi Editore, Modena, 2025.

a un monitoraggio costante. Molti Paesi hanno adottato indicazioni nazionali che raccomandano di non superare le due ore al giorno di utilizzo ricreativo. Tuttavia, nella realtà quotidiana questa soglia è ampiamente superata. Le differenze si accentuano nei fine settimana e riflettono anche le disparità socioeconomiche: in diversi Paesi (come Colombia, Nuova Zelanda, Turchia) i giovani provenienti da famiglie più abbienti hanno fino al 25% di probabilità in più di superare le due ore giornaliere rispetto ai coetanei con minori risorse; altrove, invece, l'uso intensivo è trasversale e coinvolge oltre l'80% degli adolescenti, indipendentemente dal contesto familiare (Germania, Corea, Polonia, Repubblica Ceca, Ungheria, Lettonia, Estonia).

Questo tempo-schermo protratto, sommato alle architetture persuasive delle piattaforme e alla logica della "connessione permanente", costituisce il terreno di coltura per diverse dipendenze comportamentali. Tra queste, il *gaming disorder*, riconosciuto come condizione clinica dall'OMS, si manifesta attraverso un *pattern* di gioco persistente e ricorrente, caratterizzato dalla perdita di controllo, dal crescente disinteresse verso altre attività e da una compromissione significativa delle sfere scolastiche, sociali e relazionali. Analogamente, la *social addiction* descrive il bisogno compulsivo di interagire attraverso piattaforme sociali, alimentato da meccanismi di gratificazione istantanea (*like*, commenti, visualizzazioni) che incidono sul benessere psicologico, sulla percezione del sé e sull'autostima. Tali dipendenze non producono soltanto un "dispendio di tempo", ma incidono sulla qualità delle relazioni, amplificando isolamento, ansia e forme di autopercezione distorta.

In questo *continuum* può essere collocato il fenomeno dei cosiddetti "hikikomori digitali" [17], espressione estrema dell'autoreclusione volontaria, che si traduce in un progressivo ritiro dalla vita scolastica, sociale e familiare. Nato in Giappone negli anni '80, il termine (dal verbo *hiki*, "tirare indietro", e *komoru*, "ritirarsi") descrive adolescenti o giovani adulti che si chiudono per mesi o anni nelle loro stanze, riducendo al minimo i contatti con l'esterno e sostituendoli con interazioni virtuali. In Italia si stimano tra 50.000 e 100.000 casi, con una maggiore incidenza nella fascia 11-19 anni.

Gli hikikomori non vanno intesi come un blocco statico, ma come persone immerse in una condizione di fragilità, scandita da fasi progressive: nella prima, i giovani riducono le attività esterne e manifestano assenze scolastiche intermittenti, sostituite da videogiochi o streaming compulsivo; nella seconda, si chiudono quasi totalmente nella propria stanza, mantenendo relazioni minime con i genitori e comunicazioni solo online; nella terza, si isolano del tutto,

[17] Vedi B. ROSSI, *Iperconnettività e rischio dell'autoreclusione: il fenomeno dei c.d. "hikikomori"*, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025, pp. 59-70.

rinunciando anche ai legami virtuali e correndo un rischio elevato di sviluppare patologie psichiche gravi [18].

L'analisi del fenomeno mette in luce un paradosso: la rete può funzionare sia come rifugio che come prigione, offrendo temporaneo sollievo dal disagio ma al contempo alimentando l'isolamento. In Europa si stima che circa 9 milioni di giovani siano affetti da disturbi di ansia, depressione e altre condizioni correlate alla fragilità psichica, e in Italia un adolescente su cinque dichiara uno stato emotivo alterato, mentre uno su tre prova vergogna a chiedere aiuto [19]. In questo contesto, l'autoreclusione appare come una risposta patologica a pressioni sociali, aspettative familiari e modelli estetici irraggiungibili veicolati dai social [20].

Il rischio comune a tutte queste forme di dipendenza digitale – dal *gaming disorder* alla *social addiction*, fino all'hikikomori – è quello di consolidare un circolo vizioso in cui l'ambiente online, anziché risorsa di crescita e di socialità, diventa un ambiente totalizzante che imprigiona, compromette le capacità relazionali e ostacola la costruzione di identità equilibrate.

La sfida educativa e istituzionale consiste dunque nel fornire strumenti di alfabetizzazione critica, nell'intercettare precocemente i segnali di disagio e nel costruire reti di sostegno capaci di sostenere i giovani non solo nella prevenzione, ma anche nel reinserimento sociale e scolastico, riconoscendo la complessità e la variabilità dei percorsi individuali.

2.2. Cyberbullismo e discorsi d'odio

Il cyberbullismo costituisce oggi una delle manifestazioni più pervasive e preoccupanti della violenza in rete [21]. Esso rappresenta la trasposizione e l'amplificazione digitale delle forme tradizionali di bullismo: insulti, esclusione sociale, denigrazione, diffusione di contenuti offensivi. Inseriti nello spazio

---

[18] I dati dell'ISS mostrano come, nel periodo post-pandemico, i cosiddetti "lupi solitari" siano quasi raddoppiati, passando dal 5,6% nel 2019 al 9,7% nel 2022: cfr. L. CERBARA-G. CIANCIMINO-G. CORSETTI *et al*., *Self-isolation of adolescents after Covid-19 pandemic between social withdrawal and Hikikomori risk in Italy*, in *Scientific Reports*, vol. 15, 2025.

[19] https://www.unicef.org/media/108121/file/SOWC-2021-Europe-regional-brief.pdf.

[20] Nel contesto italiano: A. VERZA, *L'hikikomori e il giardino all'inglese: inquietante irrazionalità e solitudine comune*, in *Ragion pratica*, 46, 2016, pp. 243-258.

[21] Vedi M. MONDELLO, *Odio e violenza online: il "cyberbullismo"*, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, cit., pp 85-98. G. VIGGIANI, *Il cyberbullismo: considerazioni socio-giuridiche a cinque anni dall'entrata in vigore della legge 71/2017*, in B.G. BELLO-L. SCUDIERI (a cura di), *L'odio online: forme, prevenzione e contrasto*, Giappichelli, Torino, 2022, pp. 123-136.

"onlife [22]" tali comportamenti assumono un impatto potenzialmente illimitato, poiché i contenuti digitali possono circolare indefinitamente, raggiungere un pubblico vastissimo e continuare a produrre effetti lesivi anche a distanza di tempo. La vittima, spesso un adolescente, si trova così esposta a una pressione continua, aggravata dall'impossibilità di isolare lo spazio virtuale dalla quotidianità analogica. Ne derivano conseguenze gravi sul piano psicologico e relazionale, che possono includere ansia, depressione, isolamento, ritiro scolastico, autolesionismo e, nei casi più estremi, tentativi di suicidio.

Il dato empirico conferma la diffusione capillare del fenomeno: secondo l'indagine ISTAT Nuove generazioni sempre più digitali e multiculturali (2024) [23], in Italia quasi l'85% dei giovani tra gli 11 e i 19 anni possiede almeno un profilo social. Sono proprio questi spazi a costituire il teatro principale delle condotte riconducibili al cyberbullismo. Non stupisce, quindi, che la comunità internazionale abbia progressivamente riconosciuto la necessità di garantire anche nell'ambiente digitale i diritti sanciti dalla Convenzione ONU sui diritti dell'infanzia e dell'adolescenza (1989), tra cui la libertà di espressione, la sicurezza, l'ascolto e la protezione della salute psico-fisica.

In Italia, l'intervento legislativo si è concretizzato con la l. 29 maggio 2017, n. 71, recante Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo, recentemente aggiornata dalla l. 17 maggio 2024, n. 70. L'impianto normativo non ha introdotto una nuova fattispecie penale autonoma, scelta dettata dalla consapevolezza che anche gli autori di tali condotte sono spesso minori, ma ha privilegiato strumenti di tipo preventivo, educativo e amministrativo. La legge offre una definizione ampia di cyberbullismo (art. 1, comma 2), comprendente una pluralità di condotte (dalla molestia al ricatto, dalla diffamazione al furto di identità, fino alla diffusione illecita di dati personali). Essa si fonda su due pilastri: l'istanza di oscuramento, rimozione o blocco dei contenuti, attivabile anche direttamente dal minore ultraquattordicenne (art. 2), e l'ammonimento del Questore, volto a interrompere condotte suscettibili di aggravarsi (art. 7). A tali strumenti si affianca quello che dovrebbe essere un sistema di prevenzione scolastica: istituzione di tavoli tecnici nazionali, linee di orientamento per gli istituti, designazione di un docente referente in ogni istituto, campagne di sensibilizzazione periodiche e, più di recente, la possibilità per le Regioni di attivare servizi di supporto psicologico presso le scuole.

Nonostante la portata innovativa, l'applicazione della normativa incontra criticità strutturali. Anzitutto, la difficoltà nel coinvolgere i gestori di app di

[22] L. FLORIDI, *The Onlife Manifesto*, in *Philosophy & Technology*, vol. 26, n. 2, 2013, pp. 133-141.

[23] https://www.istat.it/comunicato-stampa/indagine-bambini-e-ragazzi-anno-2023/.

messaggistica o di ambienti di gaming online, spesso scenario di abusi verbali e discriminazioni. In secondo luogo, i termini stringenti per la rimozione dei contenuti (48 ore) si scontrano con la dimensione transnazionale delle grandi piattaforme, che non hanno sede legale in Italia. Infine, l'efficacia delle misure preventive appare ridimensionata dalla scarsità di risorse economiche: i fondi disponibili per campagne informative e iniziative educative rimangono estremamente contenuti, e gli oneri organizzativi non sono accompagnati da incentivi concreti o riconoscimenti per scuole e docenti.

Un ulteriore profilo rilevante è il legame tra cyberbullismo e discorsi d'odio (*hate speech*) [24]. Molte delle condotte di cyberbullismo hanno natura eminentemente verbale: insulti, offese, *body shaming*, minacce, diffamazione. Esse si sovrappongono spesso alle dinamiche dell'hate speech, fondato su stereotipi e pregiudizi radicati che prendono di mira persone che sono ritenute appartenere a "categorie vulnerabili": minori con *background* migratorio, ragazze e giovani donne, persone LGBTQIA+, soggetti con disabilità. Le caratteristiche peculiari dell'*hate speech* digitale – percezione di anonimato o impunità, volatilità e ricontestualizzazione dei contenuti, effetto *boomerang* e transnazionalità – contribuiscono a rafforzare l'impatto lesivo e a rendere difficoltosa l'azione di contrasto [25].

Il contrasto al cyberbullismo non può basarsi solo su misure repressive o interventi individuali: è necessaria una strategia nazionale di educazione digitale, sostenuta da risorse adeguate e orientata alla prevenzione. Un approccio che coinvolga scuole, famiglie, comunità educanti e istituzioni è indispensabile per sviluppare competenze critiche e ridurre la vulnerabilità dei minori alla violenza e alla discriminazione online.

2.3. Adescamento online, esposizione a contenuti inappropriati, *sexting, reveng porn*

Tra le minacce più insidiose che caratterizzano l'ecosistema digitale vi è l'adescamento online (*child grooming*), pratica attraverso la quale un adulto instaura con un minore un rapporto apparentemente innocuo, con lo scopo di condurlo gradualmente verso una relazione di natura sessualizzata. La forza di questo fenomeno risiede nella sua natura manipolativa: la relazione viene costruita

[24] F. DI TANO, *Hate speech e molestie in rete: profili giuridici e prospettive de iure condendo*, Aracne, Roma, 2019. Si vedano anche C. BIANCHI, *Hate speech. Il lato oscuro del linguaggio*, Laterza, Bari, 2021; A. DI ROSA, *Hate speech e discriminazione: un'analisi performativa tra diritti umani e teorie della libertà*, Mucchi, Modena, 2020.

[25] Per un'ampia trattazione: B.G. BELLO-L. SCUDIERI (a cura di), *L'odio online: forme, prevenzione e contrasto*, cit.

con cura nel tempo, attraverso il ricorso a strategie di persuasione e ascolto che spesso intercettano bisogni reali del minore, quali il riconoscimento, il sostegno emotivo e il desiderio di appartenenza. L'ambiente digitale amplifica questa vulnerabilità, poiché l'anonimato e l'assenza di barriere fisiche rendono più semplice l'instaurarsi di un rapporto asimmetrico. Non a caso, il legislatore italiano ha introdotto una specifica fattispecie di reato (art. 609-*undecies* c.p.), riconoscendo l'adescamento telematico come condotta autonoma e meritevole di sanzione penale, anche prima che si traduca in un abuso fisico.

Accanto all'adescamento, un ulteriore fattore di rischio riguarda l'esposizione precoce a contenuti inappropriati. Le indagini internazionali hanno mostrato come una percentuale significativa di adolescenti si imbatta, spesso in maniera accidentale, in immagini o video sessualmente espliciti, violenti o incitanti all'autolesionismo. L'accesso ubiquo e difficilmente filtrabile della rete fa sì che tali contenuti siano raggiungibili anche al di fuori di intenzioni consapevoli, con effetti potenzialmente devastanti sul benessere psicologico e sullo sviluppo relazionale. L'esposizione ripetuta a pornografia violenta in adolescenza, ad esempio, può favorire processi di normalizzazione della violenza sessuale e rafforzare stereotipi di genere.

Un fenomeno frequentemente oggetto di attenzione è il sexting, inteso come produzione e condivisione, tra adolescenti, di testi, immagini o video a contenuto sessualmente esplicito. Se per molti giovani questa pratica può rappresentare una forma di sperimentazione affettiva e identitaria, essa comporta, al contempo, rischi elevatissimi si pensi al cyberbullismo, ai ricatti digitali (*sextortion*), che sfruttano la vulnerabilità emotiva della vittima.

La diffusione non consensuale di tali materiali può dar luogo a un ulteriore e grave fenomeno: il *revenge porn* [26] (art. 612-*ter* c.p.), cioè la diffusione intenzionale di immagini o video sessualmente espliciti senza il consenso della persona ritratta. Essere vittima di questi comportamenti comporta conseguenze psicologiche, sociali e giuridiche particolarmente drammatiche: perdita di reputazione, isolamento, depressione e nei casi più estremi tentativi di suicidio. La rapidità con cui i contenuti possono diffondersi online e la difficoltà di rimuoverli stabilmente amplificano l'impatto della violenza, rendendo la vittima potenzialmente esposta a una ri-vittimizzazione continua.

L'elemento che accomuna *grooming*, esposizione a contenuti inappropriati, sexting e *revenge porn* è la perdita di controllo da parte della persona di minore età sulla propria immagine e sul proprio spazio digitale.

Il danno non si esaurisce nell'immediato, ma si proietta nel tempo,

[26] Vedi V. BARONE, *Sessismo e tossicità nelle relazioni di genere: il "revenge porn"*, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, cit., pp. 71-84.

condizionando percorsi di vita e traiettorie identitarie. A ciò si aggiunge la difficoltà, per famiglie e istituzioni educative, di intercettare i segnali precoci di disagio: vergogna, timore di punizioni e mancanza di fiducia negli adulti di riferimento portano spesso i ragazzi e le ragazze a non denunciare quanto vissuto.

In questo scenario, la risposta deve essere duplice: da un lato, occorre affinare strumenti giuridici chiari e procedure rapide per la tutela delle vittime e la rimozione dei contenuti illeciti; dall'altro, occorre sviluppare percorsi educativi orientati a promuovere un dialogo intergenerazionale e un uso consapevole delle tecnologie. Solo una sinergia tra istituzioni, scuola, famiglia e piattaforme digitali può contribuire a prevenire queste forme di violenza e a garantire ai minori un ambiente online sicuro e rispettoso della dignità personale.

2.4. Dark web

Tra i contesti digitali che sollevano maggiori preoccupazioni si colloca il cosiddetto *dark web*, descritto come la "parte oscura" della rete e associato a pratiche illecite che possono costituire una minaccia, in particolare per i minori. Il termine viene utilizzato frequentemente in maniera generica, con rappresentazioni che tendono più a suggestionare l'opinione pubblica che a descrivere in modo accurato la complessità del fenomeno. In realtà, occorre distinguere tra le diverse stratificazioni di Internet: il *surface web*, ossia la porzione aperta e indicizzata dai motori di ricerca, cui appartengono i siti di uso quotidiano; il *deep web*, costituito da contenuti non indicizzati ma accessibili tramite credenziali e infine il *dark web*, che, pur rappresentando una frazione minima del traffico complessivo della rete, è accessibile soltanto attraverso software specifici come Tor o I2P, in grado di garantire elevati livelli di anonimato grazie a complessi meccanismi di crittografia multilivello (*onion routing*).

Le categorie di rischio possono essere ricondotte a tre dimensioni principali.

In primo luogo, la produzione e circolazione di materiale pedopornografico. Ricerche recenti hanno stimato che circa il 20% dei domini ".onion" ospiti contenuti di questo tipo [27], rendendo il *dark web* uno dei principali vettori di diffusione di immagini e video di abusi su minori. Non si tratta di un fenomeno isolato: piattaforme come Boystown, smantellata nel 2021, o Playpen, chiusa nel 2015, hanno coinvolto centinaia di migliaia di utenti, organizzati in comunità strutturate, con forum, *thread* tematici e ruoli differenziati (osservatori, utenti attivi, moderatori). Questi ambienti non si limitano allo scambio di contenuti, ma alimentano un processo di socializzazione deviata, in cui si condividono competenze tecniche, strategie di anonimizzazione e tecniche di *grooming*. Ne

[27] Scientific Reports, 2024.

risulta una vera e propria "subcultura digitale" che normalizza l'abuso e contribuisce a rafforzare la spirale di sfruttamento.

In secondo luogo, il *dark web* espone i minori a rischi connessi all'esposizione involontaria a contenuti inappropriati, sessuali o violenti. L'accesso a tali materiali può avvenire accidentalmente, soprattutto per adolescenti attratti dalla curiosità o dalla ricerca di spazi percepiti come più sicuri e anonimi. La letteratura evidenzia come la visione precoce e ripetuta di contenuti pedopornografici sia fortemente dannosa per lo sviluppo psicologico e sessuale, determinando traumi, distorsioni percettive e, in alcuni casi, aumentando la probabilità di comportamenti imitativi.

Un terzo ambito di rischio, in progressiva crescita, riguarda il coinvolgimento diretto dei minori in attività illegali. Una quota ridotta ma crescente di adolescenti, dotati di competenze digitali avanzate, utilizza il *dark web* per acquistare sostanze stupefacenti, armi da fuoco o accedere a contenuti violenti e proibiti. Le indagini internazionali mostrano come la maggior parte delle transazioni di droga avvenga in realtà tramite social network e applicazioni di messaggistica, più accessibili e meno tecnicamente complesse; tuttavia, il *dark web* resta un canale rilevante, soprattutto per gli acquisti più rischiosi.

Ancora più significativo è il crescente fenomeno dell'*hacking* giovanile: comunità presenti nel *dark web* offrono manuali, malware e opportunità di ingresso in gruppi organizzati, favorendo l'avvicinamento dei giovani alla criminalità informatica. In alcuni casi, tali competenze potrebbero essere indirizzate verso pratiche di *ethical hacking*, ma in assenza di percorsi educativi e formativi adeguati prevale il rischio di un loro impiego in contesti devianti.

Pur riconoscendo che il *dark web* non costituisca il principale spazio di adescamento – che si realizza prevalentemente su piattaforme *mainstream* di largo utilizzo da parte dei minori – esso rappresenta una zona di estrema vulnerabilità, in cui i rischi già presenti negli ambienti digitali comuni si radicalizzano e si intrecciano con dinamiche di criminalità organizzata.

La difficoltà di tracciamento e di rimozione dei contenuti rende questo ambito particolarmente critico, sollevando interrogativi urgenti sul ruolo delle istituzioni, delle famiglie e delle comunità educanti nel prevenire l'accesso dei minori a tali ambienti e nel rafforzare percorsi di consapevolezza digitale.

3. I rischi "riflessi": quando gli adulti espongono le persone di minore età

Accanto ai rischi diretti che i minori possono incontrare nella navigazione online si collocano i cosiddetti rischi "riflessi", cioè quelli derivanti dal

comportamento degli adulti e dalle dinamiche dell'economia digitale che incidono, spesso in modo inconsapevole o non intenzionale, sulla sfera di protezione dei più giovani.

In questo ambito, due fenomeni risultano particolarmente rilevanti: lo *sharenting*, ossia la pratica dei genitori che condividono in maniera sistematica immagini e informazioni sui propri figli, e il fenomeno dei *baby influencer*, bambini e adolescenti protagonisti di contenuti commerciali diffusi attraverso i social media.

3.1. Lo *sharenting*: dinamiche, implicazioni psicologiche e giuridiche

La riflessione sulla relazione tra minori e tecnologie digitali non può esaurirsi nell'analisi delle pratiche direttamente poste in essere dai ragazzi e dalle ragazze, dai giovani in senso ampio. In numerosi casi, infatti, sono gli adulti stessi – genitori, nonni, familiari, educatori – a determinare forme di esposizione indiretta, le quali incidono profondamente sulla sfera privata e identitaria dei minori. Questo fenomeno, che la letteratura ha iniziato a indagare con maggiore sistematicità negli ultimi anni, rende evidente come la vulnerabilità digitale dei bambini non dipenda soltanto dalle loro competenze o dalle loro scelte, ma anche da comportamenti e decisioni che appartengono al mondo adulto.

Il passaggio storico dai social network ai social media ha accentuato questa dinamica: le piattaforme sono oggi, prima di tutto, spazi di produzione/consumo di contenuti e di autorappresentazione, in cui la narrazione personale diviene facilmente narrazione familiare. In tale cornice lo *sharenting* [28] – la condivisione pubblica in rete, da parte di genitori o altri familiari, di immagini, video, informazioni e dati personali dei figli – rappresenta l'esempio paradigmatico dei "rischi riflessi": il minore risulta esposto non per propria iniziativa, ma come effetto dell'autorappresentazione adulta.

Le motivazioni che spingono allo *sharenting* sono molteplici e in parte legittime: coltivare legami a distanza, costruire e mantenere comunità di pari (altri genitori), cercare supporto informativo o emotivo, archiviare ricordi di crescita. A queste spinte si aggiungono driver tipici dell'ecosistema piattaforme: i meccanismi di *engagement* (*like*, commenti, visualizzazioni) che quantificano l'accettazione sociale e incentivano la continuità delle pubblicazioni; in una quota non trascurabile di casi, la monetizzazione dei contenuti, che avvicina la narrazione familiare alla creator economy e può sfociare in forme organizzate di

[28] Vedi M. BALBINOT, *Il rischio della (sovra)esposizione: genitori in rete e sharenting*, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, cit., pp.125-142.

esposizione (fino ai *baby influencer*, dei quali ci si occuperà poco più avanti). In breve, l'identità genitoriale mediata viene performata anche attraverso l'immagine dei figli, selezionando tratti e situazioni conformi agli obiettivi (riconoscimento, appartenenza, status, aiuto), con l'effetto di produrre per i minori tracce digitali perenni non decise da loro.

Accanto a potenziali opportunità (connessione con reti di sostegno, capitale sociale, scambio di esperienze), il bilancio presenta rischi sostanziali e differenziati.

Sul piano della privacy, lo *sharenting* erode il controllo del minore sui propri dati e sulla propria immagine, anticipando una identità digitale eterodiretta e talora stigmatizzante.

Sul piano criminologico, la letteratura segnala il rischio di furto d'identità (anche nella forma di *digital kidnapping* [29]), il riuso illecito di immagini in circuiti pedopornografici o su canali poco presidiati, nonché la facilitazione del *grooming* tramite elementi identificativi e di geolocalizzazione disseminati nei post.

Vi sono poi effetti diacronici: i materiali condivisi in età infantile possono riemergere in fasi successive, alimentando bullismo/cyberbullismo e pregiudicando la reputazione in momenti delicati (preadolescenza, ingresso scolastico superiore, prime esperienze lavorative, assunzione di incarichi pubblici e istituzionali).

Sul piano giuridico, il quadro di tutele è articolato ma presenta zone grigie. A livello internazionale, la Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza (1989) tutela la vita privata e riconosce il diritto del minore ad essere ascoltato; a livello europeo, la Carta dei diritti fondamentali (2001) e il GDPR (2016) affermano la protezione dei dati personali, il principio di trasparenza e il diritto all'oblio. Tuttavia, l'eccezione per l'"uso personale/domestico" e l'incertezza circa la pubblicità effettiva dei contenuti social (anche da profili "privati") rendono difficile l'applicazione automatica delle norme. Alcuni ordinamenti hanno iniziato a intervenire in modo più mirato: ad es. la Francia, con la l. n. 1266/2020 sull'uso commerciale dell'immagine dei minori; in Italia esistono diverse proposte legislative per limitare lo *sharenting* e regolare i proventi derivanti dall'immagine del minore, oltre a rafforzare le condizioni per l'esercizio del diritto all'oblio. In giurisprudenza prende corpo l'idea che la diffusione dell'immagine del minore sia atto di straordinaria amministrazione, per cui è richiesto quanto meno il consenso congiunto dei genitori, con valorizzazione della volontà del minore proporzionata a età e maturità.

Di qui la necessità di un *duplice cambio di paradigma*.

---

[29] Il termine *digital kidnapping* indica una pratica illecita che consiste nel prelevare e riutilizzare online foto o video di minori (solitamente condivisi dai genitori o da altri adulti sui social media) senza alcun consenso, spesso con finalità distorsive o criminali.

Sul versante *regolativo*, occorre un bilanciamento più chiaro tra libertà di espressione familiare e interesse superiore del minore, con limiti effettivi alla monetizzazione della sua immagine, obblighi di trasparenza per le piattaforme e procedure rapide per la rimozione/cancellazione dei contenuti lesivi.

Sul versante *educativo*, serve promuovere uno "*sharenting* responsabile": competenze tecniche minime (gestione del pubblico, strumenti anti-ricondivisione quando disponibili, preferenza per canali ristretti nelle comunicazioni familiari), ma soprattutto una cultura del consenso che soggettivizzi i minori, coinvolgendoli – per quanto possibile – nelle decisioni sulla loro immagine, anche in età precoce con modalità adeguate.

In questa prospettiva, famiglie, scuole e piattaforme ma anche istituzioni sono chiamate a una *responsabilità condivisa*: solo così è possibile ridurre i rischi riflessi senza negare i legittimi bisogni di relazione, appartenenza e memoria che animano la vita familiare online.

3.2. Il fenomeno dei *baby influencer*: tra sfruttamento commerciale e diritto all'infanzia

Se lo *sharenting* rappresenta la versione "ordinaria" di un'esposizione che può sembrare innocua ma che rischia di compromettere la costruzione dell'identità digitale del minore e di generare contenziosi familiari, i *baby influencer* costituiscono una declinazione "professionale" e spesso economicamente rilevante di questa sovraesposizione [30]. Bambini e adolescenti vengono progressivamente coinvolti in attività di promozione commerciale, acquisendo visibilità e popolarità attraverso canali digitali e piattaforme social. In questi casi, le persone di minore età, gli adolescenti, non sono soltanto destinatari passivi di contenuti, ma diventano veri e propri protagonisti della *creator economy* [31], con conseguente esposizione a dinamiche economiche, contrattuali e mediatiche che li assimilano a figure professionali.

La questione solleva interrogativi giuridici di rilievo: fino a che punto è lecito assimilare il lavoro digitale di un minore alle forme tradizionali di

[30] Per un primo inquadramento: M. DI FRANCESCO, *Baby influencer e sharenting: il quadro attuale tra incertezze e tentativi di riforma*, in TH. CASADEI-V. COLOMBA (a cura di), *Società digitale e mondi professionali*, Bonomo, Bologna, 2025, pp. 179-183.

[31] La *creator economy* è l'ecosistema economico, sociale e professionale che si è sviluppato attorno ai creatori di contenuti digitali, ovvero individui che producono, distribuiscono e monetizzano contenuti, prodotti o servizi tramite piattaforme online. Sul lavoro degli utenti e sulle varie forme di valore estratte dalle piattaforme digitale, si veda, più in generale, F. OLIVERI, Machina mundi. *Per una regolazione democratica dei poteri digitali*, Mucchi editore, Modena, 2025, pp. 114-115.

prestazione lavorativa? Quali tutele economiche e sociali devono essere garantite? Quali limiti occorre porre alla monetizzazione dell'immagine infantile? La risposta normativa, ancora frammentaria, segnala l'urgenza di una riflessione sistematica sulla protezione dei minori in un contesto in cui i confini tra gioco, creatività, sfruttamento lavorativo e commerciale diventano sempre più sfumati.

Si tratta di bambini che, sotto la direzione di genitori o tutori, collaborano con aziende per la promozione di prodotti e servizi, generando contenuti che raggiungono milioni di visualizzazioni. La loro popolarità digitale, lungi dall'essere un semplice passatempo, si traduce in introiti significativi che pongono interrogativi cruciali sulla gestione dei proventi, sul consenso informato del minore e, più in generale, sul riconoscimento dei suoi diritti fondamentali.

Il quadro normativo italiano, tuttavia, si presenta frammentario e arretrato rispetto alla rapidità con cui questi fenomeni si sviluppano. Non esiste una disciplina organica che regoli l'attività dei *baby influencer*, né un sistema chiaro che stabilisca limiti all'impiego dei minori in campagne digitali o che disciplini la destinazione dei guadagni. La giurisprudenza si è trovata più volte a colmare tali vuoti, ad esempio nelle controversie relative alla pubblicazione di immagini di minori senza il consenso dell'altro genitore, oppure nei casi – sempre più frequenti – in cui i figli, divenuti maggiorenni, hanno agito giudizialmente contro i propri genitori per la lesione della propria riservatezza e identità digitale.

Una prima risposta istituzionale è stata la proposta di l. n. 1771, presentata alla Camera nel marzo 2024, che intende aggiornare la l. n. 977/1967 sul lavoro minorile. La proposta estende espressamente le tutele previste per le attività artistiche e di spettacolo anche all'ambito delle piattaforme digitali, imponendo contratti regolari laddove l'attività assuma un carattere continuativo o superi determinate soglie di reddito. Inoltre, stabilisce che i proventi derivanti dall'attività online dei minori siano gestiti da un curatore speciale nominato dal tribunale, con versamenti su conti vincolati fino al compimento della maggiore età. Particolarmente rilevante, in questo contesto, è anche l'introduzione del diritto all'oblio per i ragazzi dai quattordici anni in su, che consente loro di richiedere la rimozione delle immagini e dei contenuti condivisi senza consenso.

Il fenomeno dei *baby influencer* e dello *sharenting* pone dunque questioni delicate che vanno oltre la semplice gestione economica. Si tratta, più profondamente, di fenomeni che toccano la costruzione dell'identità personale e digitale delle persone di minore età, l'esercizio della responsabilità genitoriale e il bilanciamento tra libertà di espressione, esigenze commerciali e tutela dei diritti fondamentali.

Alla luce di tali criticità, il diritto è chiamato a colmare un vuoto regolativo che rischia di tradursi in sfruttamento per i soggetti più fragili, in condizioni di vulnerabilità. Ma accanto all'intervento legislativo, si impone una riflessione più ampia che coinvolge le piattaforme digitali – chiamate a introdurre codici

di autoregolamentazione specifici – e le comunità educative, che devono promuovere nei genitori una maggiore consapevolezza delle conseguenze delle proprie scelte online.

In assenza di un'educazione digitale diffusa e di controlli effettivi, infatti, ogni norma rischia di rimanere inefficace, incapace di contrastare un fenomeno che si alimenta della popolarità e della viralità proprie della cultura digitale contemporanea.

Infine, l'attenzione ai rischi riflessi richiama anche la responsabilità delle istituzioni e delle piattaforme digitali. Non si tratta soltanto di educare gli adulti a un uso più consapevole dei social media, ma di costruire un sistema multilivello di protezione che coinvolga legislatori, scuole, mondi sportivi, comunità educanti e imprese tecnologiche.

Come hanno sottolineato alcune studiose [32], la sicurezza dei minori nello spazio digitale richiede un *approccio integrato*, capace di combinare la responsabilità individuale dei genitori con la regolazione pubblica e con la predisposizione, da parte delle piattaforme, di strumenti effettivi di tutela.

In questo senso, la questione dei rischi riflessi mette in luce una verità fondamentale: la cittadinanza digitale dei minori non si costruisce isolatamente, ma dipende in larga misura dall'ambiente che li circonda e dalle scelte collettive che regolano l'ecosistema digitale e che intendono la sicurezza digitale come un bene pubblico [33].

4. Il progetto SAFELY: educazione, consapevolezza e prevenzione

4.1. Inquadramento: contesto e obiettivi

Con l'intento di offrire strumenti per queste sfide è maturato il progetto SAFELY – Social media Awareness For Education and Legal Youth, elaborato

---

[32] M. STOILOVA-R. NANDAGIRI-S. LIVINGSTONE, *Children's understanding of personal data and privacy online. Systematic evidence mapping*, in *Information, Communication, & Society*, vol. 24, 2021, n. 4, pp. 557-575.

[33] Sul punto: R. BRIGHI-P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *Federalismi.it*, 2021, 21, pp. 18-42. Cfr., anche, R. BRIGHI, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in TH. CASADEI-S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 75-87; R. BRIGHI, *Cybersicurezza e Intelligenza Artificiale. Un'analisi critica*, in *Biolaw Journal*, 1, 2024, pp. 111-124; P.G. CHIARA-R. BRIGHI, *La dimensione della "resilienza" nel diritto UE della cybersicurezza*, in *Ragion Pratica*, 2024, 2, pp. 405-426.

presso il CRID dell'Università di Modena e Reggio Emilia e finanziato nell'ambito del PNRR.

Il progetto SAFELY (PI: Prof. Thomas Casadei) promuove la consapevolezza digitale concentrandosi, in particolare, sulle giovani generazioni. Ideato e progettato all'interno del CRID – Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità dell'Università di Modena e Reggio Emilia è finanziato nell'ambito dello Spoke 8 "Risk Management and Governance" (coordinatore il Prof. Michele Colajanni) della Fondazione SERICS – Security and Rights in CyberSpace e rientra all'interno del più ampio Progetto EcoCyber in sinergia con il WP 'Regole per la società futura' (coordinatrice la Prof.ssa Raffaella Brighi).

La mappatura delle minacce (dipendenze comportamentali e autoreclusione, cyberbullismo e *hate speech*, adescamento) ha mostrato come l'ecosistema digitale tenda a amplificare vulnerabilità preesistenti e, al contempo, a generare rischi inediti legati ad anonimato, persistenza dei contenuti e mercatizzazione dei dati. Ne discende l'esigenza di interventi sistemici che affianchino alla regolazione giuridica percorsi strutturati di educazione, prevenzione e consapevolezza, rivolti *in primis* a minori, famiglie, scuole e comunità educanti.

4.2. Attività principali

L'attività di SAFELY si è articolato lungo più direttrici complementari, che riflettono l'approccio interdisciplinare del progetto: ricerca e analisi, mappatura dei fenomeni legati a comportamenti a rischio online (hate speech, sextortion, cyberbullismo, disinformazione, dipendenze); elaborazione di strumenti didattici – produzione di materiali destinati a docenti e studenti; disseminazione e formazione – organizzazione di seminari e laboratori sia in presenza che online, rivolti a scuole secondarie e a università, con l'obiettivo di stimolare un dialogo tra ricercatori, insegnanti, famiglie e studenti; divulgazione – creazione di un ecosistema comunicativo accessibile che include podcast, interviste, video brevi, guide divulgative e un portale web dedicato (https://www.safely.unimore.it); eventi – conferenze e giornate di studio che consolidano i risultati raggiunti, favorendo il confronto istituzioni e istituti scolastici.

Diversi sono stati gli strumenti messi a punto.

4.3. La Mappa dei comportamenti dannosi online

Nella prospettiva di promuovere una maggiore consapevolezza dei rischi digitali e di dotare educatori, famiglie e studenti di strumenti chiari e condivisi, è emersa con forza la necessità di costruire un linguaggio comune, capace di

ridurre la distanza tra le definizioni tecnico-giuridiche e le esperienze concrete vissute dai giovani utenti.

La Mappa dei comportamenti dannosi online, uno dei primi esiti del progetto SAFELY [34], nasce precisamente con questo obiettivo: offrire un ponte semantico che renda accessibili concetti complessi, favorendo il dialogo non solo tra esperti e non addetti ai lavori, ma anche e soprattutto tra generazioni. In tal senso, essa si configura come uno strumento che consente agli adulti di comprendere meglio l'universo linguistico e culturale delle nuove generazioni, e, allo stesso tempo, ai ragazzi di collocare le proprie esperienze digitali all'interno di categorie condivise e riconosciute.

La mappa raccoglie 70 voci, ordinate alfabeticamente, ciascuna delle quali affronta un comportamento a rischio online. Per ogni voce vengono fornite: una descrizione sintetica del fenomeno; un'analisi dei rischi connessi; l'indicazione dei comportamenti da adottare per difendersi nonché i riferimenti giuridici essenziali. Questa articolazione la rende uno strumento didattico e formativo, utile per l'alfabetizzazione critica nei percorsi scolastici e di educazione civica digitale, e al contempo un dispositivo preventivo, poiché permette a genitori, docenti e operatori di riconoscere precocemente i segnali di rischio e di orientarsi verso risposte adeguate.

L'impianto alfabetico non rappresenta solo un criterio ordinativo, ma una precisa scelta metodologica: facilita la consultazione e trasforma la mappa in un vocabolario operativo, fruibile nella quotidianità dei contesti educativi. In tal modo, essa non si limita a registrare fenomeni emergenti, ma li traduce in un lessico condiviso, favorendo così un dialogo intergenerazionale che riduce i fraintendimenti e rafforza la capacità delle comunità educanti di affrontare con strumenti adeguati la complessità del digitale.

4.4. Guide divulgative

Accanto alla mappa, SAFELY ha avuto tra i suoi esiti strumenti di intervento, bibliografici, la guida "Giovani in rete. Guida per un uso consapevole delle tecnologie" (Giappichelli, 2025), pensata per tradurre le conoscenze specialistiche in un linguaggio chiaro, pratico e immediatamente utilizzabile da studenti, famiglie, insegnanti e, in generale, cittadinanza interessata.

La guida affronta, in capitoli tematici, i principali rischi digitali, proponendo consigli pratici, schede riassuntive e percorsi di approfondimento.

A completamento della guida cartacea, il progetto ha sviluppato una sorta di "ecosistema multimediale" che comprende: podcast: interviste a esperti, testimonianze di studenti, riflessioni su casi concreti; video brevi e interviste:

[34] https://www.safely.unimore.it/mappa-dei-comportamenti-dannosi/.

destinati alla condivisione su piattaforme social, per raggiungere un pubblico ampio di giovani; eventi divulgativi e formativi: giornate di studio, workshop scolastici e seminari pubblici, che hanno coinvolto attivamente scuole, università, associazioni e istituzioni territoriali.

Questi strumenti, una aggiornata "cassetta degli attrezzi", hanno la funzione di moltiplicare i canali di comunicazione e di avvicinare i giovani nei loro stessi ambienti digitali, offrendo messaggi di prevenzione e consapevolezza con linguaggi e format a loro familiari.

Inoltre, il progetto evidenzia un aspetto cruciale: la lotta ai rischi digitali non può esaurirsi nella sola dimensione repressiva o tecnologica, ma deve includere un investimento sistematico in educazione e prevenzione, capace di promuovere *cittadinanza digitale*, *responsabilità condivisa* e *partecipazione consapevole*.

5. Verso una responsabilità condivisa e partecipata: strategie educative per un uso consapevole e sicuro delle tecnologie

5.1. L'educazione digitale: dall'alfabetizzazione digitale alla cittadinanza digitale

Se in una prima fase l'educazione digitale è stata concepita prevalentemente come alfabetizzazione tecnica – ossia come acquisizione di competenze di base per l'utilizzo di dispositivi e software – oggi emerge con chiarezza la necessità di ampliare questa prospettiva verso la formazione di una vera e propria cittadinanza digitale [35]. Non basta, infatti, saper utilizzare uno strumento: occorre imparare a esercitare in rete i diritti fondamentali, a rispettare regole di convivenza e a riconoscere i rischi che l'ecosistema digitale comporta.

La cittadinanza digitale implica dunque *competenze critiche* (capacità di distinguere tra informazione e disinformazione), *etiche* (responsabilità verso gli altri utenti, rispetto della privacy, contrasto all'*hate speech*), e *partecipative* (uso delle tecnologie per contribuire a processi democratici e di inclusione sociale).

In questa prospettiva, l'educazione digitale si configura come una dimensione trasversale, che attraversa certamente l'istruzione scolastica ma che si estende anche al contesto familiare, comunitario, sportivo, promuovendo un uso consapevole, sicuro e orientato all'autonomia.

---

[35] Vedi C. SEVERI, *I patti educativi digitali: fiducia, cooperazione e diritti per un'educazione digitale consapevole*, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, cit., pp. 165-180.

5.2. Buone pratiche per la famiglia e per la scuola

La costruzione di un ambiente digitale sicuro passa inevitabilmente attraverso pratiche educative quotidiane, capaci di armonizzare regole e libertà.

In ambito familiare, la condivisione di regole chiare sull'uso dei dispositivi – ad esempio stabilire momenti di disconnessione durante i pasti o limitare l'uso notturno degli smartphone – favorisce un rapporto equilibrato con la tecnologia. Non si tratta di imporre divieti rigidi, ma di promuovere una cultura della gradualità e dell'accompagnamento, che rispetti le fasi di crescita e lo sviluppo psicologico dei minori.

Anche la scuola è chiamata a svolgere un ruolo determinante: non solo integrando il digitale nella didattica in modo creativo e critico, ma anche affrontando esplicitamente i rischi connessi, come il cyberbullismo, il *sexting* o la disinformazione.

Le buone pratiche si collocano quindi in una prospettiva di coerenza educativa, in cui scuole e famiglie operano in sinergia, evitando messaggi contraddittori che rischiano di disorientare i più giovani.

5.3. La necessità di un dialogo intergenerazionale

Uno degli aspetti più delicati dell'educazione digitale è la distanza tra le generazioni.

Gli adulti, pur dotati di maggiore esperienza di vita, spesso faticano a comprendere linguaggi, dinamiche e piattaforme utilizzate dai giovani, che al contrario vivono in un ecosistema digitale come parte integrante della propria identità. Tale divario non è soltanto tecnico, ma anche culturale: ciò che per i ragazzi è una normale modalità di socializzazione, per i genitori può apparire come un terreno estraneo e potenzialmente pericoloso.

Promuovere un dialogo intergenerazionale significa allora creare spazi di reciproco ascolto, nei quali adulti (anche anziani) e giovani possano confrontarsi apertamente sulle opportunità e sui rischi del digitale. Questo confronto riduce la diffidenza, accresce la fiducia reciproca e permette di costruire un lessico condiviso, in grado di tradurre concetti complessi in esperienze comprensibili a entrambe le generazioni ma anche di affrontare rischi e situazioni comuni. In tal senso, il dialogo intergenerazionale diventa non solo una strategia educativa, ma anche una pratica finalizzata alla coesione sociale.

5.4. Il ruolo delle "comunità educanti": la formazione di insegnanti e genitori, la partecipazione dei giovani

La costruzione di quella che può essere definita una "comunità educante digitale" [36] non può prescindere da una duplice prospettiva: da un lato, il rafforzamento delle competenze di insegnanti e genitori, dall'altro, il coinvolgimento attivo dei giovani come co-protagonisti dei processi formativi.

La formazione degli adulti rappresenta il primo passo imprescindibile. Senza una conoscenza di base delle dinamiche digitali e delle insidie che esse comportano, i genitori rischiano di oscillare tra eccessiva permissività e divieti repressivi, mentre i docenti possono trovarsi disarmati di fronte alle nuove forme di disagio che emergono nelle classi in cui si trovano ad operare, un'esperienza, questa, che riguarda più in generale chi è impegnato in ruoli educativi. Sono dunque necessari occasioni e percorsi formativi continui, capaci di integrare elementi tecnici con una solida consapevolezza pedagogica, psicologica e giuridica, così da trasformare insegnanti, genitori, figure educative in riferimenti credibili e competenti.

Parallelamente, i giovani stessi devono essere messi nella condizione di assumere un ruolo attivo nella costruzione di pratiche digitali responsabili. La loro partecipazione non può ridursi a un ascolto passivo delle regole elaborate dagli adulti, ma deve tradursi in spazi di co-progettazione, nei quali studenti e studentesse contribuiscano con il proprio sguardo, le proprie esperienze e i propri linguaggi.

In questa prospettiva, la comunità educante digitale si configura come un ecosistema aperto e plurale, capace di integrare competenze tecniche e sensibilità educative, di bilanciare diritti e responsabilità, di riconoscere le vulnerabilità ma anche le potenzialità dei più giovani. L'obiettivo non è soltanto proteggere i minori dai rischi della rete, ma promuovere una cittadinanza digitale che valorizzi la loro capacità di contribuire attivamente al bene comune, anche attraverso forme di impegno sociale e civile che trovano negli ambienti digitali nuovi e potenti strumenti di espressione.

5.5. Prevenzione dei rischi e valorizzazione delle opportunità

Infine, l'educazione digitale non può limitarsi a prevenire i pericoli: deve anche saper riconoscere e valorizzare le straordinarie opportunità offerte dalle tecnologie. L'accesso all'informazione, la possibilità di sviluppare creatività, la

[36] Vedi G. GASPARINI, *Per una comunità educante digitale: la formazione di insegnanti e genitori, la partecipazione dei giovani*, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, cit., pp. 153-164.

partecipazione civica online, la collaborazione e la cooperazione in rete rappresentano risorse preziose per la crescita personale e sociale [37].

Prevenzione e valorizzazione devono procedere insieme: da un lato, contrastare fenomeni quali quelli esaminati in precedenza, come cyberbullismo, *hate speech*, *sexting*, *sextortion*, *revenge porn*, dipendenza da schermi e autoreclusione, pratiche di disinformazione ecc.; dall'altro, promuovere esperienze positive, come progetti di educazione civica digitale, attività di *coding* e robotica educativa, forme di volontariato e cittadinanza attiva online, realizzazione di iniziative e campagne di promozione della cultura del rispetto e dell'educazione alle differenze.

In questo equilibrio risiede la vera sfida: fare del digitale non un semplice strumento, ma un ambiente formativo aperto, nel quale le persone di minore età, gli adolescenti e i giovani possano essere cittadini e cittadine consapevoli, responsabili e solidali.

Al fine di favorire questi processi, che possono far aumentare la consapevolezza sulle questioni digitali, a cominciare dalla sicurezza on line, occorrono baricentri e sperimentazioni, spazi in cui sia possibile segnalare e riconoscere rischi e minacce, nonché prevenirne le cause, ma anche incontrare e diffondere buone pratiche di utilizzo dei dispositivi e degli strumenti informatici e tecnologici.

6. Dallo studio all'azione: lo Sportello informativo SAFELY

6.1. Lo Sportello come eredità e prosecuzione del progetto

Nel corso delle attività del progetto SAFELY, soprattutto in seguito a dialoghi e confronti sia con insegnanti e figure educative sia con studenti e studentesse, è maturata l'idea di costituire uno Sportello informativo che possa favorire il dialogo e il confronto su situazioni problematiche collegate all'uso della rete e degli strumenti digitali, nonché su comportamenti e condotte messi in atto negli ambienti e nelle comunicazioni digitali.

Le finalità di un'iniziativa di questo tipo possono essere molteplici.

In primo luogo, fornire strumenti informativi e pratici per riconoscere e gestire situazioni di rischio, sia per coloro che possono essere loro malgrado oggetto o vittime di determinati comportamenti sia per coloro che possono in una qualche modalità essersi ritrovati ad agire pratiche con effetti potenzialmente deleteri o, anche, gravi.

---

[37] Un riferimento imprescindibile per questo tipo di approccio resta R. SENNETT, *Insieme. Rituali, piaceri, politiche della collaborazione*, Feltrinelli, Milano, 2016.

In secondo luogo, promuovere, anche mediante incontri e dialoghi in presenza o on line, un utilizzo consapevole e responsabile delle tecnologie, nel rispetto della sicurezza, della privacy e, più ampiamente, del "benessere digitale" [38]. Siffatta finalità potrebbe connettersi ad altre iniziative come i patti educativi digitali [39] o i corsi di alfabetizzazione informatica pensati anche per adulti e persone anziane [40].

Uno sportello di questo tipo, istituito in ambito accademico, avrebbe, per inciso, anche il merito di perseguire, in modo inedito e originale, la cosiddetta "terza missione" dell'università, nel caso specifico declinata nella sua funzione sociale, di servizio alla comunità.

In quest'ottica, in terzo luogo, lo sportello potrebbero costituire uno spazio di ascolto aperto anche alla cittadinanza, ossia a chi si ritrovi ad avere dubbi rispetto a determinate situazioni o in seguito a inconvenienti che la rete e l'uso delle tecnologie possono determinare: lo sportello potrebbe in tal caso indirizzare a enti e soggetti preposti ad un intervento o anche solo rassicurare nel caso le questioni poste non abbiano il carattere della gravità o di un possibile reato.

6.2. A disposizione del mondo scolastico ed educativo, ma anche sportivo

Siffatto sportello, più in particolare, potrebbe svolgere una funzione di sostegno e di orientamento per il mondo scolastico e per i soggetti che in esso

---

[38] Un esempio significativo è rappresentato dal progetto "Benessere Digitale – scuole", promosso dall'Università di Milano-Bicocca. Cfr. *Le sfide educative e sociali della connessione permanente*, intervista al Prof. Marco Gui, in TH. CASADEI-V. BARONE-B. ROSSI (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, cit., pp. 199-206.

[39] Sul territorio modenese, sia consentito menzionare il gruppo di lavoro "Patti educativi digitali e uso consapevole della rete" (https://www.crid.unimore.it/site/home/attivita/laboratori-e-gruppi-di-lavoro/articolo1065068599.html), nato in seno all'Officina Informatica DET – Diritto Etica Tecnologie, istituita presso il CRID – Centro di Ricerca interdipartimentale su Discriminazioni e vulnerabilità, Unimore. Il gruppo di lavoro, coordinato dalla Prof.ssa Barbara G. Bello, dalla Dott.ssa Claudia Severi, dal Dott. Marco Mondello e dal Dr. Casimiro Coniglione, collabora con la rete "Patti Digitali. Per un'educazione di comunità all'uso della tecnologia", promuovendo il modello dei patti educativi digitali mediante incontri nelle scuole e in varie realtà associative e istituzionali del territorio. Per un approfondimento: TH. CASADEI, *Patti educativi digitali: una possibile risposta alle sfide tecnologiche*, in *Sociologia del diritto*, 2, 2025 (dossier su "Adolescenti nell'epoca della trasformazione digitale: un approccio sociologico, normativo e culturale").

[40] Nel "Decreto Legislativo Anziani" (15 marzo 2024, n. 29. *Disposizioni in materia di politiche in favore delle persone anziane, in attuazione della delega di cui agli articoli 3, 4 e 5 della legge 23 marzo 2023*, n. 33 [24G00050])40, il Capo V è dedicato alle "Misure in materia di alfabetizzazione informatica e facilitazione digitale".

operano studenti e insegnanti, ma anche per chi con esso è chiamato a interagire come famiglie e genitori.

Gli istituti scolastici sono ormai da tempo dotati di figure di sostegno psicologico e di sportelli di ascolto, nonché di team contro il cyberbullismo composti da insegnanti. Questi ultimi sovente si ritrovano ad operare senza avere strumenti di accurata comprensione dei fenomeni che vengono portati alla loro attenzione, sia sul versante tecnologico sia, soprattutto, sul versante giuridico e normativo. Ma anche le figure preposte al sostegno psicologico in alcuni casi possono necessitare di approfondimenti sul fronte legislativo o essere alla ricerca di buone pratiche magari già realizzate in altri contesti. Poter attingere ad un patrimonio di informazioni e di strumenti utili per far fronte a situazioni problematiche potrebbe costituire un esempio di quel "sapere collaborativo" di cui non solo pare esserci grande bisogno nei contesti formativi ma di cui c'è precisa necessità se si intende cogliere la sfida educativa e istituzionale posta dall'imponente sviluppo delle nuove tecnologie e dalla connessione permanente dei giovani e, al contempo, promuovere dialogo intergenerazionale e responsabilità condivise.

In tale scenario di cooperazione tra mondi diversi uniti dall'intenzione di far fronte a sfide complesse, un ambito di ulteriore sperimentazione, confronto e anche raccordo potrebbe riguardare il coinvolgimento anche del mondo sportivo.

Se infatti l'obiettivo è quello di mettere a punto e diffondere strumenti concreti a disposizione della comunità educante – composta da famiglie, scuole, enti locali, associazioni e servizi territoriali – finalizzati a promuovere una cultura del rispetto, della sicurezza, della cura e della legalità anche nello spazio digitale, mediante la costruzione di un quadro condiviso di regole, volte a prevenire l'insorgenza di comportamenti irrispettosi, aggressivi o, appunto, addirittura penalmente rilevanti, nessun ambito in cui si trovano ad agire persone di minore età e giovani può essere lasciato in disparte.

La promozione di una cultura dell'educazione digitale che sia condivisa, partecipata e radicata nella responsabilità individuale e collettiva pare dunque potersi proficuamente espandere anche in ambiti sino ad oggi rimasti a latere come quello sportivo [41].

[41] In questa direzione si sta muovendo l'esperienza condotta dal gruppo di lavoro "Patti educativi digitali e uso consapevole della rete" del CRID che, a partire da un accordo di collaborazione con il CSI – Centro Sportivo Italiano di Modena, ha in programma una serie di iniziative che andranno a coinvolgere genitori, educatori ed educatrici dei mondi dello sport, ragazzi e ragazze impegnati nella pratica sportiva, nonché rappresentanti istituzionali.

6.3. La cooperazione tra competenze e esperienze professionali: verso una clinica legale digitale?

Lo sportello in questione potrebbe offrire ulteriori opportunità anche sul piano dell'aggiornamento delle competenze e dell'organizzazione della didattica universitaria.

Come si è sottolineato in diversi passaggi della trattazione, il bisogno di formazione chiama in causa tutte le generazioni e richiama l'importanza di dialoghi intergenerazionali, oltre che tra diverse istituzioni. Coloro che operano nell'ambito delle professioni dell'istruzione ed educative, e dunque anche all'interno del mondo accademico, sono sempre più chiamati al ricorso agli strumenti tecnologici per veicolare i contenuti formativi ma anche a prendere piena consapevolezza di nuove questioni e nuovi rischi dinanzi ai quali può ritrovarsi la relazione educativa, al di là delle discipline di insegnamento: come si è visto, dalle pratiche di autoreclusione dei cosiddetti "hikikomori" al cyberbullismo, dai discorsi d'odio alla misoginia on line fino ad arrivare ai casi di adescamento di minori (*child grooming*), pedopornografia e *revenge porn* [42].

Quelli richiamati costituiscono problemi molto concreti per le nuove generazioni e per le famiglie, ma anche per chi quotidianamente, in ambito professionale, con esse deve relazionarsi.

Le prime generazioni di adolescenti "datificati" [43] segnalano la centralità acquisita dalla *cittadinanza digitale*, una questione che riguarda, in realtà, tutte le età e che si presenta come cruciale anche nel comparto delle amministrazioni pubbliche.

Anche su questo versante, quindi, si combinano nuove esigenze da parte di soggetti in condizioni di vulnerabilità (specificamente *digitale*) e il bisogno di aggiornamento delle competenze (e della capacità di comprendere le situazioni) per chi opera all'interno del sistema dei servizi.

Per queste ragioni lo Sportello potrebbe, dopo una fase sperimentale d'avvio, assumere l'assetto di una "clinica legale" [44] specificamente dedicata agli ambienti digitali e agli atti e ai comportamenti che in essi si manifestano.

---

[42] Per un approfondimento sia consentito rinviare a V. COLOMBA-TH. CASADEI, *Prefazione. Professioni e società digitale: una sfida aperta*, in TH. CASADEI-V. COLOMBA (a cura di), *Società digitale e mondi professionali*, cit., pp. 10-11.

[43] Si veda, in merito, M. MARTONI, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *Federalismi.it*, 1, 2020, pp. 119-136.

[44] Per una presentazione di questo tipo di esperienze, ormai consolidate anche in Italia si rinvia a: F. DI DONATO-F. SCAMARDELLA, *Il metodo clinico-legale. Radici teoriche e dimensioni pratiche*, Editoriale scientifica, Napoli, 2016; A. SCIURBA, *Le cliniche legali italiane e la risignificazione del diritto*, in *Rivista di filosofia del diritto*, n. 2, 2019, p. 257 ss.

Come è stato opportunamente segnalato, questi contesti impegnano gli studenti in situazioni reali, promuovendo un apprendimento esperienziale del diritto e favorendo così lo sviluppo di una perizia di tipo tecnico-pratico [45], quanto mai necessaria nell'affrontare questioni, situazioni, problemi, dilemmi posti dai comportamenti in rete e negli ambienti digitali.

Le attività qui svolte, anche in forma esperienziale e laboratoriale, agevolano una approfondita comprensione del diritto, l'intuizione e anche – aspetto non secondario – la gestione delle emozioni in relazione ai casi, attraverso il contatto diretto con le persone comuni e, con riferimento alla quotidianità digitale, con le situazioni che esse possono incontrare nelle loro esperienze in rete o mediate dalla rete.

Questo approdo consentirebbe scambi e interazioni a vari livelli: non solo tra docenti, studentesse e studenti universitari con operatori e professionisti del diritto ma anche tra costoro e gli insegnanti nonché, sotto la supervisione di questi ultimi, gli studenti e le studentesse, i quali potrebbero così interfacciarsi con i loro quasi coetanei e scoprire così un mondo nuovo che può offrire loro possibili risposte e soluzioni o anche solo comprensione rispetto a situazioni che possono generare disorientamento, sconforto e, in taluni casi, anche sofferenza.

[45] B.G. BELLO, *Formazione giuridica e didattica del diritto nel mondo che cambia*, in AA.VV., *Diritto e diritti nel mondo che cambia*, Editoriale scientifica, Napoli, 2024, pp. 39-61, p. 54.

Finito di stampare nel mese di novembre 2025
nella Stampatre s.r.l. di Torino
Via Bologna, 220