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].

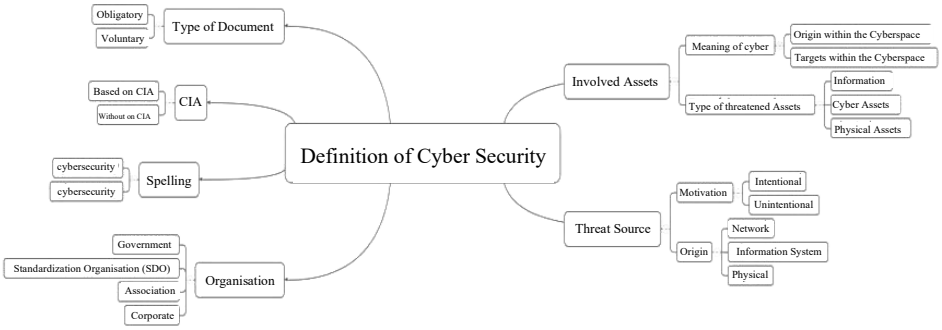
---

[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.