La governance della cybersecurity nell'era dell'intelligenza artificiale tra quadro normativo europeo e nazionale*

Stefania Ardito

Sommario

1. L'evoluzione normativa in materia di *cybersecurity*

La progressiva interconnessione di reti[1] e sistemi informativi[2] ha condotto alla formazione di un tessuto infrastrutturale unitario, la cui funzionalità costituisce il presupposto imprescindibile per l'esercizio di funzioni pubbliche e per la continuità dei processi produttivi. La disponibilità e l'inte-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Il presente articolo riprende, integra e approfondisce il contributo dell'*Autrice* intitolato "*Tutela della cybersecurity e dell'intelligenza artificiale*" e destinato al volume "*Le regole dei dati e dell'intelligenza artificiale. Dal GDPR alla Legge 132/2025*" a cura di G. Cassano ed E. Prosperetti.

[1] In termini tecnici, per reti (*network*) si intendono le reti di comunicazione elettronica, cioè collegamenti fisici e logici che permettono la trasmissione di dati, incluse le infrastrutture fisiche (mezzi di comunicazione, nodi e dispositivi di rete) e i protocolli che supportano le connessioni. Sono le reti a permettere la trasmissione dei dati fra dispositivi o sistemi e sono componenti essenziali delle infrastrutture digitali.

[2] In termini tecnici, i *sistemi informativi* sono dispositivi, *software*, processi e dati che, connettendosi alle reti, consentono di trattare, memorizzare, elaborare, recuperare, utilizzare e trasmettere le informazioni digitali, supportando servizi e applicazioni.

grità delle infrastrutture digitali[3] sono condizioni strutturali del funzionamento dei settori vitali per l'economia e la società,[4] al punto da configurare una dipendenza di questi ultimi, che, da una prospettiva regolatoria, impone un ripensamento delle categorie tradizionali della sicurezza, integrità, affidabilità e resilienza.

Gli utenti (cittadini, pubbliche amministrazioni e organizzazioni private), generano, raccolgono, elaborano e conservano quantità crescenti di informazioni, inclusi dati personali, attraverso un insieme eterogeneo di dispositivi interconnessi, che spaziano dai *computer* agli *smartphone*, fino ai sistemi IoT.[5] [6] La loro capillare diffusione ha moltiplicato la superficie di esposizione ai rischi informatici. Tale situazione è stata aggravata dall'integrazione di sistemi, modelli e strumenti basati sull'AI generativa nelle tecnologie di uso quotidiano, e, dunque, ha aumentato la probabilità che si verifichino incidenti alle reti e ai sistemi; siano questi dovuti ad attacchi o a guasti, malfunzionamenti tecnici o a un errore umano.[7] L'impiego dell'AI generativa - ancorché amplifichi i benefici in termini di efficienza, produttività e capacità predittiva - introduce inevitabilmente nuove vulnerabilità connesse alla produzione di informazioni *unsafe*. L'informazione sicura diventa, pertanto, un obiettivo primario delle normative che regolamen-

[3] In termini tecnici, le infrastrutture digitali costituiscono l'insieme integrato di reti, sistemi informativi, ovvero di componenti *hardware* e *software*, servizi *cloud*, sistemi di supporto (come la sicurezza, l'alimentazione, la gestione operativa) necessari per garantire il funzionamento sicuro, continuo e affidabile dell'ecosistema digitale, in particolare per le attività critiche delle organizzazioni pubbliche e private e la fornitura dei servizi. Questo insieme di componenti fisiche, logiche e di servizio permette l'erogazione dei servizi digitali.

[4] Considerando 97 NIS2.

[5] Considerando 96 NIS2.

[6] Inclusi i prodotti con elementi digitali, ovvero «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente» (art. 3, punto 1, CRA).

[7] Considerando 96 NIS2.

tano il digitale[8] e delle *policy* di *data governance*[9], le quali integrano studi[10] e strategie di *risk management*[11] facendo propria la regola «*the higher the risk, the stricter the rules*».[12] La stessa disponibilità di dati e contenuti digitali, infatti, se non governata, può trasformarsi in un vettore di rischi sistemici per l'economia, i diritti fondamentali e la sicurezza collettiva. L'interruzione o la compromissione delle reti e dei sistemi informativi sui quali si fondano queste attività produrrebbe conseguenze negative non solo per gli utilizzatori diretti, ma anche per soggetti terzi (*non-users*) a causa della natura sistemica e interconnessa del rischio informatico.[13]

---

[8] Tra le principali fonti che a livello unionale disciplinano l'informazione in ambito digitale, secondo prospettive differenti, si annoverano, *inter alia*, il Regolamento (UE) 2016/679 (GDPR), la Direttiva (UE) 2022/2555 (NIS2), il Regolamento (UE) 2022/2554 (DORA), il Regolamento (UE) 2022/2065 (Digital Services Act – DSA), il Regolamento (UE) 2024/1689 (AI Act), il Regolamento (UE) 2024/2847 (Cyber Resilience Act – CRA), nonché il Regolamento (UE) n. 910/2014 (eIDAS), come modificato dal Regolamento (UE) 2024/1183 (eIDAS2) in materia di identificazione elettronica e servizi fiduciari. A livello nazionale, si richiamano, non esaustivamente, il Perimetro di Sicurezza Nazionale Cibernetica, il Codice dell'Amministrazione Digitale (CAD), introdotto con d.lgs. 82/2005 e successivamente oggetto di interventi integrativi e di modifica, nonché la recente l. 132/2025 in materia di intelligenza artificiale, entrata in vigore il 10 ottobre 2025.

[9] J.M. Balkin, *Free speech in the algorithmic society: Big data, private governance, and new school speech regulation*, in *UC Davis Law Review*, 51, 2018, 1149 ss.

[10] La letteratura di *management* parla di informazioni "*unsafe*" in quanto «errate, opache o potenzialmente dannose», dunque irrispettose dei principi fondanti della sicurezza delle informazioni (c.d. *CIA triad*), mentre sarebbero da considerarsi *cybersafe* quelle informazioni «*correct, open, benignant*». Per maggiori chiarimenti si veda lo studio P. Spagnoletti-R. Baskerville*, Safe and Unsafe Information: Managing Risks in the Era of Generative Artificial Intelligence,* in *Proceedings of the 35th European Safety and Reliability Conference (ESREL2025) and the 33rd Society for Risk Analysis Europe Conference*, 2025, 1934 ss.

[11] A. Burgess-A. Alemanno-J. Zinn (a cura di), *Routledge handbook of risk studies*, London, 2016; B.T. Sørensen, *Digitalisation: an Opportunity or a Risk?*, in *Journal of European Competition Law & Practice*, 6, 2018, 349 ss.

[12] Si veda European Council, *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*, in *consilium.europa.eu*, 2 febbraio 2024.

[13] Si pensi, a titolo esemplificativo, agli attacchi di disinformazione *online* attuati mediante tecniche coordinate di manipolazione informativa veicolate dalle piattaforme digitali, con ricadute concrete sulla libertà di espressione e di informazione. In tale contesto, reti di propagazione strategiche - *bot*, account falsi, *cluster* tematizzati, reti di amplificazione automatica - operano come moltiplicatori e veicolano contenuti *unsafe*, nella misura in cui frammentano il discorso pubblico, polarizzano opinioni e generano asimmetrie informative. Si veda A. Gullo-I. Pasquetto-G. Riotta-N. Apolito, *Come individuare e contrastare operazioni coordinate di disinformazione in Italia*, in *esteri.it*, 2023; J.L. Vargas Valdez, *Study on the role of social media and the internet in democratic development*, Council of Europe (Venice Commission), in *venice.coe.int*, 2018; ENISA, *Foreign Information Manipulation and Interference (FIMI) and cybersecurity - Threat Landscape*, in *enisa.europa.eu*, dicembre 2022.

L'espansione esponenziale delle attività svolte *online* non solo ha moltiplicato la quantità dei dati generati e scambiati, ma ha altresì innalzato il livello qualitativo e la granularità dell'informazione, consentendo di ricostruire profili progressivamente più dettagliati e potenzialmente invasivi della sfera privata e professionale delle persone.[14] Negli ultimi anni, la *cyber awareness*, istituzionale[15]e normativa, ha conosciuto un'accelerazione senza precedenti traducendosi in un progressivo rafforzamento dei quadri regolatori[16] e della cooperazione pubblico-privata.[17] L'incremento di eventi *cyber*[18] che si registrano ogni anno è riconducibile, *prima facie*, a una crescita quantitativa delle minacce,[19] ma riflette anche l'evoluzione degli strumenti tecnici, normativi e di cooperazione che consentono ai CSIRT (*Computer Security Incident Response Team*) europei[20], incluso quello italiano[21], un monitoraggio continuo, processi di *information sharing*[22] e, pertanto, una rileva-

[14] ENISA, *Threat Landscape*, in *enisa.europa.eu*, settembre 2024.

[15] D. Eckert, *40 Years of European Digital Policies. Forgotten Lessons*, Cham, 2024.

[16] 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, 2024, 106071 s.

[17] A. Gullo, *Compliance*, in *Archivio Penale*, 1, 2023, 1 ss.

[18] Per evento *cyber* si intende «Qualsiasi evento osservabile in una rete o in un sistema informativo». Si veda ACN, *Domini della cybersicurezza - Event, Threat and Incident Management*, su *acn.gov.it*.

[19] Nel solo primo semestre 2025, l'Italia ha registrato 1.549 eventi *cyber* (+53% rispetto al primo semestre 2024), che hanno colpito 2.367 soggetti (in diversi casi più volte), di cui 346 con un impatto confermato (+98% rispetto allo stesso periodo del 2024) e dunque con conseguenze tangibili "nel mondo reale". Si veda ACN, *Operational Summary del 1° semestre 2025*, in *acn.gov.it*.

[20] Ai sensi dell'art. 15.1, lett. a), Decreto NIS2 «è l'organo preposto alle funzioni di gestione degli incidenti di sicurezza informatica per i settori, i sottosettori e le tipologie di soggetti di cui agli allegati I, II, III e IV, conformemente a modalità e procedure definite dal CSIRT stesso».

[21] I dati vengono raccolti dal CSIRT Italia. Il CSIRT Italia è stato istituito con il d.lgs. 65/2018 che ha recepito la Direttiva NIS1 e definito compiti e funzioni. Successivamente, il D.P.C.M. 8 agosto 2019 ne ha disciplinato organizzazione e funzionamento presso il Dipartimento delle informazioni per la sicurezza (DIS). Con il d.l. 14 giugno 2021, n. 82, il CSIRT è stato trasferito presso l'ACN, assumendo la denominazione di CSIRT Italia e configurandosi come punto di contatto nazionale unico per la gestione e la notifica degli incidenti *cyber*. Nel quadro attuale, ulteriormente rafforzato dalla normativa NIS2, il CSIRT Italia è l'articolazione tecnico-operativa di ACN, destinatario delle notifiche di tutti gli incidenti *cyber* che si verificano sul territorio nazionale e che coinvolgono i soggetti individuati e disciplinati dalla normativa, tra cui il Perimetro di Sicurezza Nazionale Cibernetica, l. 90/2024, e d.lgs 138/2024, che recepisce la Direttiva NIS2. Inoltre, svolge un ruolo centrale nella prevenzione, nel monitoraggio e nella risposta agli incidenti, operando quale nodo fondamentale del sistema nazionale ed europeo di gestione del rischio *cyber*.

[22] F. Serini, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche.*

zione più capillare e proattiva di vulnerabilità, minacce e attacchi *cyber*. [23]

Verso una definizione di cybersicurezza integrata?, in questa *Rivista*, 3, 2023, 1 ss.

[23] L'art. 23 Direttiva NIS2 afferma che «*Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority … of any incident that has a significant impact on the provision of their services*». L'*Operational Summary* di ACN, relativo al mese di gennaio 2026, registra un aumento del numero di incidenti *cyber* segnalati dalle organizzazioni nei diversi settori disciplinati. Questo riflette, da un lato, una maggiore consapevolezza del rischio da parte delle organizzazioni e, dall'altro, la progressiva adozione di corrette procedure di notifica. Nel contesto italiano i risultati in termini di *compliance* appaiono particolarmente significativi se si considera che le organizzazioni rientranti nel perimetro normativo - sia unionale sia nazionale - sono di dimensione e tipologia variegata. Inoltre, come noto, esse non partivano da livelli omogenei di conoscenza e maturità tecnologica (cfr., ad esempio, i Report Eurostat o ISTAT annuali in ambito Imprese e ICT antecedenti e successivi al periodo Covid-19). In questo processo evolutivo, un ruolo rilevante è svolto dall'emersione di obblighi di *compliance* sempre più strutturati contenuti nelle normative ma anche dalle iniziative di indirizzo e supporto di natura non cogente, ma funzionalmente connesse all'attuazione degli obblighi previsti per gli Stati membri quali, ad esempio, quelli della Direttiva NIS2 che richiede, *inter alia*, di: (*i*) adottare una strategia nazionale in materia di *cybersecurity*, che comprenda politiche per la sicurezza della catena di approvvigionamento; (*ii*) la gestione delle vulnerabilità; (*iii*) l'educazione e la sensibilizzazione in materia, applicate in combinato con le necessità derivanti dalla normativa domestica.
Tra le iniziative non cogenti portate avanti da ACN si annoverano strumenti operativi, anche con funzione di coordinamento tra normativa unionale e nazionale, quali la "tassonomia *cyber*": linee guida finalizzate all'adozione di un lessico comune a livello nazionale, esigenza particolarmente rilevante alla luce della derivazione unionale e della prevalente lingua inglese della materia.
Le linee guida sulla *constituency* del CSIRT Italia che individuano l'insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta, al fine di prevenire e gestire eventi e incidenti di sicurezza informatica. In tale documento, la principale distinzione tra i soggetti - obbligati, non obbligati e "ulteriori" - si fonda sulla sussistenza o meno di obblighi di notifica degli incidenti rilevanti per la sicurezza nazionale, nonché sul diverso grado di responsabilità strategica attribuito loro da leggi specifiche. In particolare, rientrano tra i soggetti obbligati quelli a cui sono conferiti specifici obblighi di sicurezza e notifica da fonti normative settoriali, quali: il d.l. 105/2019 (soggetti PSNC), il Codice delle Comunicazioni Elettroniche (CCE) - d.lgs. 259/2003 (Operatori TELCO) e della l. 90/2024 (soggetti individuati dall'articolo 1, co. 1). Si veda ACN, *La constituency del CSIRT Italia Definizione dei soggetti parte della constituency*, in acn.gov.it, 31 luglio 2024. Si noti che il documento si rivolge inoltre ai soggetti individuati ai sensi del d.lgs. n. 65/2018 (operatori di servizi essenziali e fornitori di servizi digitali), che ha recepito la direttiva NIS1, oggi superata e ampliata dalla Direttiva NIS2, la quale estende significativamente il perimetro soggettivo ai 18 settori individuati a livello europeo. Accanto ai soggetti obbligati, le linee guida includono anche i «soggetti operanti nei settori critici senza obbligo di notifica», che, pur non essendo formalmente individuati dal legislatore, sono considerati parte della *constituency* in ragione della loro operatività in ambiti strategici. Infine, vi rientrano gli "ulteriori soggetti", ossia quelli non sottoposti ad obblighi di notifica e operanti in settori diversi da quelli per i quali tali obblighi sono previsti, ai quali il CSIRT Italia continua a fornire servizi di base. Nel complesso, il documento evidenzia come l'operatività integrata e continuativa dell'insieme dei soggetti coinvolti sia considerata essenziale a livello

Tuttavia, gli sviluppi tecnologici, geopolitici e sociali, al pari, contribuiscono a ridefinire costantemente il panorama *cyber* ampliando la superficie di attacco, introducendo nuove sfide alla sicurezza informatica[24] e dinamiche di rischio più sofisticate, che incidono sui dati raccolti dalle autorità nazionali, tra cui, in Italia, l'Agenzia per la Cybersicurezza Nazionale (ACN). In tale contesto, la *cybersecurity*[25] dimostra una peculiare capacità di adattamento, derivante dalla sua natura intrinsecamente multidisciplinare, che le consente di rispondere alla complessità strutturale dei fenomeni digitali. Ne consegue che istituzioni e organizzazioni sono chiamate a esercitare una responsabilità condivisa nella prevenzione e gestione degli incidenti *cyber*, assumendo obblighi di protezione[26] che si estendono oltre la dimensione meramente tecnica[27] e incidono direttamente sulla tutela degli interessi giuridici[28], inclusi quelli delle persone[29], che vivono nella cosiddetta «società del rischio».[30]

A partire dalla Direttiva NIS1 del 2016[31] - primo atto normativo europeo

nazionale per il mantenimento di funzioni rilevanti «per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese, nonché per evitare pregiudizi alla sicurezza nazionale» necessitando forme di partnership pubblico-private. Pur richiedendo un aggiornamento alla luce delle più recenti evoluzioni normative, il documento costituisce ancora uno strumento utile per comprendere la logica sistemica e inclusiva della gestione degli incidenti *cyber* a livello nazionale, anche oltre il perimetro dei soggetti formalmente obbligati.

Come ultimo documento, si richiama, infine, ACN, *Guida alla notifica degli incidenti*, in acn.gov.it, 26 luglio 2024 dove viene definito un "testo unico" delle istruzioni per i diversi soggetti, pubblici e privati, tenuti per legge alla notifica degli incidenti, che, benché antecedente alla NIS2 e privo di efficacia vincolante, ha contribuito a rendere effettivi gli obblighi strategici, di gestione del rischio e di notifica degli incidenti favorendo il coordinamento e la standardizzazione delle pratiche di gestione e segnalazione per rafforzare la consapevolezza e la capacità operativa delle organizzazioni nazionali.

[24] "L'insieme delle attività volte a proteggere reti e sistemi informativi, gli utenti e tutte le persone coinvolte, contro le minacce informatiche». Così art. 2, lett. r), d.lgs 138/2024 e art. 2, punto 1, Regolamento (UE) 2019/881.

[25] In alcuni atti dell'UE, nelle traduzioni ufficiali in lingua italiana è possibile trovare anche il termine "cibersicurezza" o "cybersicurezza", come nel caso dell'AI Act, delle Direttive NIS1 e NIS2, del Cybersecurity Act e del CRA.

[26] M. Pietrangelo, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista italiana di informatica e diritto*, 6(2), 2024, 13 ss.

[27] R. Brighi-P. G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *Federalismi.it*, 8 settembre 2021.

[28] L. Picotti, *Cybersecurity: quid novi?*, in *Diritto di Internet*, 1, 2020, 11 ss.

[29] P.G. Chiara, *Towards a right to cybersecurity in EU law? The challenges ahead*, in *Computer Law & Security Review*, 53, 2024, 105961 ss.

[30] U. Beck, *Risk society. Towards a new modernity*, Londra, 1992.

[31] Direttiva (UE) 2016/1148 del Parlamento europeo e del consiglio del 6 luglio 2016

di carattere generale in materia di sicurezza delle reti e dei sistemi informativi – la produzione normativa europea si è progressivamente intensificata[32] andando a delineare due macro-filoni normativi complementari,[33]che impongono, ai soggetti interessati, obblighi di *cybersecurity*.[34] Il primo filone, definibile normativo-strategico, è volto alla protezione e alla resilienza[35] delle reti e dei sistemi informativi[36]. Esso includeva la Direttiva NIS1, successivamente sostituita dalla Direttiva NIS2[37] (di seguito NIS2), recepita in Italia mediante il d.lgs. 138/2024 (Decreto NIS2)[38], che attualmente ne fa parte, imponendo obblighi armonizzati di gestione del rischio *cyber* e doveri di notifica ai soggetti essenziali e importanti individuati a livello nazionale. Si affianca, a quanto precede, la Direttiva (UE) 2022/2557 sulla

recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[32] Con un'accelerazione notevole dopo il periodo della pandemia da Covid-19.

[33] La normativa *cyber* è estremamente trasversale e multidisciplinare e in questo contesto si richiameranno solo le normative ad applicazione più generalizzata ma per una rapida consultazione del quadro normativo europeo si consideri l'*overview of EU legislative landscape* offerta da ENISA, *Report on the State of the Cybersecurity in the Union*, in *enisa.europa.eu*, 2024.

[34] F. Teichmann-B.S. Sergi, *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in *Computer Law & Security Review*, 59, 2025, 106209 ss.

[35] Per "sicurezza dei sistemi informatici e di rete" si intende «la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi» (art. 6, punto 2, Direttiva NIS2).

[36] Per "sistema informativo e di rete" si intende: (*i*) una rete di comunicazione elettronica ai sensi dell'art. 2, c. 1, lettera vv), del d.l. 259/2003; (*ii*) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; (*iii*) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri (*i*) e (*ii*), per il loro funzionamento, uso, protezione e manutenzione. Si veda l'art. 2, c.1, lett. p), Decreto NIS2, in allineamento con l'art. 6, punto 1, Direttiva NIS2 ed all'art. 1 D.P.C.M. 81/2021 Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informatici e servizi informatici (c.d. DPCM 2) – si noti che quest'ultimo è stato aggiornato dal DPCM 111/2025, ma le modifiche principali riguardano l'aggiornamento dell'Allegato A, con la definizione di nuove macrocategorie di incidenti da segnalare.

[37] 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).

[38] Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

resilienza dei soggetti critici (CER) recepita mediante il d.lgs. 134/2024, che arricchisce l'architettura regolatoria estendendo la logica della resilienza alla dimensione fisica delle infrastrutture, per fronteggiare minacce fisiche e antropiche, oltre a quelle digitali. Completa il quadro il Regolamento (UE) 2022/2554 (DORA), che si configura come *lex specialis* rispetto alla Direttiva NIS2, ma con una verticalizzazione ancora più stringente applicabile al settore finanziario.[39]

Il secondo macro-filone riguarda le normative che si occupano di certificazione e standardizzazione della *cybersecurity* di determinati prodotti ICT, che mirano a stabilire un livello uniforme di fiducia, sicurezza e interoperabilità nel mercato digitale europeo, attraverso la creazione di schemi armonizzati di valutazione. Dette normative richiedono processi di *compliance* finalizzati a verificare che i prodotti rispettino i requisiti minimi fissati dagli *standard* di settore, così da attestare il livello di sicurezza e l'affidabilità informatica del prodotto, garantendone al contempo «autenticità, idoneità e integrità[40] sotto il profilo della sicurezza informatica»[41]. Tra la normativa attualmente applicabile assume particolare rilievo il Cybersecurity Act[42] (successivamente emendato)[43], che impone l'adozione di schemi di certificazione europei per prodotti, servizi e processi ICT, inclusi i "*managed security services*"[44], introducendo altresì *l'European common criteria-based cybersecuri-*

---

[39] Commissione europea, *Comunicazione C (2023) 6068, Orientamenti sull'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva (UE) 2022/2555 (direttiva NIS2)*, in *eur-lex.europa.eu*, 18 settembre 2023.

[40] Si ritiene importante chiarire che Autenticità e Integrità sono due concetti interconnessi fondamentali in materia. Rispettivamente sono la capacità di garantire che le informazioni e i sistemi informativi siano non alterati, e dunque che i dati e le fonti informative siano ciò che affermano di essere (verificate e affidabili), mentre, l'integrità garantisce l'assenza di modifiche non autorizzate nel tempo.

[41] L'affermazione è ormai condivisa in materia, ma per una panoramica si veda S. Poletti, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in questa *Rivista*, 2, 2023, 398 ss.

[42] Regolamento (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, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[43] European Council, *Cybersecurity package: Council adopts new laws to strengthen cybersecurity capacities in the EU*, in *consilium.europa.eu*, 2 dicembre 2024.

[44] "Servizi prestati a un terzo consistenti nello svolgimento di attività, o nella fornitura di assistenza per tali attività, legate alla gestione dei rischi in materia di cybersecurity, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica». Così l'art. 1, punto 2, lett. b), Regolamento (UE) 2025/37 del Parlamento e del Consiglio del 19 dicembre 2024 che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti.

ty certification scheme (EUCC).[45] Il più recente Regolamento (UE) 2024/2847 Cyber Resilience Act (CRA), entrato in vigore nel dicembre 2024, altrettanto rilevante, diversamente, troverà piena applicazione a partire dall'11 dicembre 2027. Il CRA stabilisce requisiti obbligatori di *cybersecurity* per i prodotti con componenti digitali, sia *hardware* che *software*, prevedendo che i medesimi debbano essere *secure by design* e *by default* da vulnerabilità e minacce informatiche per il loro intero ciclo di vita.

A queste due macro aree di derivazione unionale si aggiunge un terzo livello di intervento, di carattere nazionale, istituito con il d.l. 105/2019 e suoi decreti attuativi[46] (Decreto Perimetro), convertito con modificazioni dalla l. 133/2019, che ha comportato la creazione di un Perimetro di Sicurezza Nazionale Cibernetica (PSNC) finalizzato a garantire un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici da cui dipendono l'esercizio di funzioni essenziali dello Stato e la prestazione di servizi essenziali per attività civili, sociali o economiche fondamentali.

La matrice esclusivamente domestica della normativa è dovuta alla competenza esclusiva degli Stati membri in materia di sicurezza nazionale, come previsto dall'art. 4, par. 2, Trattato sull'Unione Europea (TUE).

Il PSNC è composto da un insieme di organizzazioni, pubbliche e private, che esercitano una funzione o assicurano un servizio essenziale dello Stato (c.d. soggetti perimetro o soggetti PSNC).[47] Esse sono individuate da decreti attuativi, a seconda del settore strategico, sulla base dei criteri di gradualità[48] e dell'analisi del rischio.[49] Le reti, i sistemi informativi, i servizi e i prodotti ICT identificati e comunicati da tali entità sono critici in quanto «dal malfunzionamento, interruzione, anche parziali, ovvero utilizzo

---

[45] Regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024 recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

[46] D.l. 105/2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica (c.d. Decreto Perimetro).

[47] Soggetti «da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero assicura la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche» e che «l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici» (art.1, c. 1, Decreto Perimetro).

[48] L'identificazione dei soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC) è disciplinata dal D.P.C.M. 131/2020, in attuazione dell'articolo 1, comma 2, del d.l. 105/2019. Tale processo si fonda su criteri procedurali e su un principio di gradualità, che tiene conto del potenziale pregiudizio (entità) per la sicurezza nazionale derivante dal malfunzionamento, dall'interruzione o dall'uso improprio di reti, sistemi informativi e servizi ICT.

[49] Art.1. c. 2, Decreto Perimetro.

improprio, potrebbe derivare un pregiudizio per la sicurezza nazionale»[50]. Per questo motivo il PSNC prevede il potere del Presidente del Consiglio dei ministri di disporre la loro disattivazione, parziale o totale, in caso di rischio grave e imminente per la sicurezza nazionale.
I soggetti perimetro hanno obblighi di sicurezza quali l'analisi dei rischi relativi a beni, servizi e funzioni essenziali e l'applicazione di misure di sicurezza elevate,[51] nonché la notifica degli incidenti,[52] al fine di proteggere le infrastrutture vitali da attacchi *cyber* che potrebbero comprometterle. Tali doveri, se disattesi, comportano il rischio dell'irrogazione delle sanzioni previste dell'art. 9 Decreto Perimetro.
Al PSNC è seguita la creazione dell'architettura istituzionale nazionale, definita innanzitutto dal d.l. 82/2021 che ha, *inter alia*, istituito l'ACN quale autorità centrale di coordinamento.[53] Si inserisce, successivamente, la l. 90/2024, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di contrasto ai reati informatici,[54] che amplia il perimetro soggettivo degli obblighi di notifica rispetto al PSNC, introducendo altresì misure di coordinamento tra le amministrazioni pubbliche e nuove funzioni. In particolare, l'articolo 1, c. 1, l. 90/2024 estende gli obbliga di notifica degli incidenti *cyber* un ampio insieme di amministrazioni pubbliche e operatori di servizi essenziali a livello territoriale e locale, tra cui le amministrazioni centrali dello Stato,[55] le regioni, le province autonome,

[50] Art.1, c.1, Decreto Perimetro.

[51] Si tratta di obblighi che discendono da un combinato disposto di norme. Si veda S. Mele, *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. Cassano–S. Previti (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, 186; S. Poletti, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, cit.

[52] La lista deli incidenti da notificare è stata recentemente aggiornata dal DPCM 4 giugno 2025, n. 111 Regolamento recante modificazioni all'allegato A al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81.

[53] Si veda l'art. 1, c. 1, punto 1, d.l. 82/2021 recante Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'ACN definisce la cybersicurezza 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 altresì la resilienza».

[54] Per una visione di insieme sulla l. 90/2024 recante Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, si veda S. Mele, *La L. 90/2024 sulla Cybersicurezza in G.U.: tutti gli adempimenti per P.A. e società private,* in *altalex.com*, 3 luglio 2024; G. Fiorinelli, *I "perimetri penali" di cybersicurezza dopo la legge n. 90/2024: dissimmetrie intra-sistematiche ed extra-sistematiche nella tutela penale dei sistemi informatici e telematici di rilevanza pubblica*, in *Cybersicurezza*, 1, 2025, 71 ss.

[55] Individuate ai sensi dell'articolo 1, c. 3, l. 196/2009

le città metropolitane, i comuni di maggiori dimensioni[56] o capoluogo, nonché specifici operatori nei settori del trasporto pubblico e della sanità. La disciplina si estende altresì alle società *in house* dei suddetti enti, qualora operino in ambiti rilevanti, quali i servizi informatici, il trasporto pubblico, la gestione delle acque reflue e dei rifiuti, evidenziando un approccio funzionale basato sulla rilevanza dei servizi erogati.
Sotto il profilo degli obblighi ai sensi dell'art. 1, c. 2, la normativa prevede un meccanismo di notifica che si articola in una segnalazione iniziale (*early warning*), da effettuarsi senza ritardo e comunque entro 24 ore dalla conoscenza dell'incidente, seguita da una notifica completa entro 72 ore contenente tutti gli elementi informativi disponibili, seguendo le fasi previste dal Decreto Perimetro ed in linea anche con la logica europea.
La legge introduce, inoltre, obblighi organizzativi rilevanti, imponendo ai soggetti interessati di dotarsi di una struttura dedicata alla cybersicurezza, se non già presente, e di individuare un referente quale punto di contatto unico con l'ACN, con funzioni di coordinamento e gestione del rischio *cyber* all'interno dell'amministrazione.[57]
La legge 90/2024 ha anticipato alcuni profili poi sistematizzati nel decreto di recepimento della Direttiva NIS2.

2. L'approccio *risk-based* della normativa in materia di *cybersecurity* e di intelligenza artificiale

Le fonti di derivazione unionale che disciplinano le materie connesse alla digitalizzazione articolano, nelle rispettive previsioni normative, approcci differenziati fondati sul modello c.d. *risk-based*. Questo emerge chiaramente dalla lettura delle disposizioni in materia di *cybersecurity*, di intelligenza artificiale (AI Act), di protezione dei dati personali (General Data Protection Regulation - GDPR) e di servizi digitali (Digital Services Act – DSA). Tali normative impongono ai loro destinatari specifici obblighi di *governance* del rischio. Si tratta di una valutazione che viene realizzata attraverso sistemi di gestione del rischio, ovvero mediante un insieme di metodologie, modelli e processi finalizzati a prendere decisioni razionali basate su potenziali opportunità o minacce future.[58] Studi evidenziano come tale approccio

[56] Con popolazione superiore a 100.000 abitanti.

[57] Per ulteriori chiarimenti sulla *ratio* e sulle altre modifiche apportate dalla legge si veda il *Dossier* del Centro Studi della Camera dei Deputati e del Senato della Repubblica, *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici,* 22 maggio 2024.

[58] G. De Gregorio-P. Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 59(2), 2022.

consente di prioritizzare ed indirizzare la *compliance* in modo proporzionato al rischio effettivo.[59]

Nella normativa *cyber* rivolta alla protezione delle infrastrutture critiche, l'adozione di programmi di gestione del rischio si configura quale obbligo prodromico imprescindibile. La *ratio* sottesa è quella di mitigare la probabilità che un evento *cyber*[60] possa determinare effetti pregiudizievoli sull'operatività dell'organizzazione, sugli *asset* critici[61] e sui servizi essenziali, con conseguenze che si ripercuotono sulle persone e sulla sicurezza pubblica. A tal fine, le organizzazioni pubbliche e private, individuate dalla normativa, sono tenute a sviluppare una mappatura completa delle attività e dei servizi suscettibili di incidere negativamente sulle reti e sui sistemi informativi connessi, traducendo tale analisi in *policy* di *risk assessment*[62]. Tali obblighi di *governance* si estendono, conseguentemente, alla predisposizione di misure di sicurezza,[63] proporzionate alla gravità del rischio rilevato, e all'osservanza degli obblighi di notifica degli incidenti all'autorità competente (in Italia, ACN).[64] La gestione del rischio implica controlli continui, processi di *audit* e obblighi di adeguamento;[65] in caso di violazioni, è prevista l'irrogazione di sanzioni pecuniarie.

In modo analogo, ma non identico, la normativa che regolamenta la *cyber* resilienza[66] dei prodotti con elementi digitali[67] - questi ultimi qualificati

---

[59] *Ibid.*

[60] "Qualsiasi evento osservabile in una rete o in un sistema informativo»; così ACN, *Domini della cybersicurezza - Event, Threat and Incident Management*, cit.

[61] I soggetti «predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica» trasmettendo tali elenchi all'ACN ai sensi dell'art.1, c. 2, lett. b), Decreto Perimetro.

[62] Art. 21, par. 2, lett. a), Direttiva NIS2; art.1, c. 3, lett. b), Decreto Perimetro.

[63] In particolare, per gli obblighi di adozione delle misure di sicurezza in capo ai soggetti Perimetro il riferimento è il Capo III -Misure di sicurezza del D.P.C.M. 14 aprile 2021, n. 81.

[64] Considerando 97, NIS2; art.1, c. 3, lett. a), Decreto Perimetro.

[65] R. Baskerville-P. Spagnoletti-J. Kim, *Incident-centered information security: Managing a strategic balance between prevention and response*, in *Information & Management*, 51(1), 2014, 138 ss.

[66] Nella traduzione ufficiale dell'UE in lingua italiana viene usato il termine "ciberresilienza", infatti il CRA è anche denominato "legge sulla ciberresilienza".

[67] Ai fini dell'individuazione dell'ambito di applicazione del Cyber Resilience Act (CRA), un prodotto con elementi digitali (c.d. prodotto digitale) rientra nella disciplina del Regolamento qualora siano soddisfatte tre condizioni cumulative. In primo luogo, il prodotto deve integrare la definizione di *product with digital elements*, ossia includere *software* o *hardware* in grado di elaborare dati e di connettersi, direttamente o indirettamente, a reti o dispositivi. Tali prodotti comprendono sia i prodotti finali che i componenti immessi separatamente sul mercato. In secondo luogo, esso deve essere messo a disposizione del

come importanti o critici ai sensi del CRA - introduce un modello di gestione del rischio fondato su requisiti orizzontali di sicurezza, parametrati al grado di rischio associato alla funzione del prodotto e al potenziale impatto sistemico derivante da una sua compromissione. La disciplina relativa all'immissione nel mercato dei prodotti con elementi digitali si fonda su un insieme articolato di obblighi in capo agli operatori economici e, soprattutto, ai fabbricanti, riguardanti le fasi di progettazione, sviluppo e produzione, nonché di adozione di processi strutturati di gestione delle vulnerabilità per l'intero periodo di utilizzo previsto del prodotto (art. 1). Nel contesto del CRA, l'attenzione del legislatore europeo si sposta dalla sicurezza delle reti e dei sistemi, alla sicurezza del prodotto in quanto tale, imponendo che questo sia immesso sul mercato, *inter alia*: (*i*) privo di vulnerabilità sfruttabili[68] note, (*ii*) con una superficie di attacco limitata[69] e (*iii*) in modo tale da non costituire una fonte di rischio per utenti e dati personali, né per altri prodotti, reti e servizi, inclusi i soggetti disciplinati dalla normativa NIS2 e le relative *supply chain*.[70]

mercato UE, secondo la nozione propria del diritto dell'Unione. In terzo luogo, la sua finalità d'uso prevista o ragionevolmente prevedibile deve comportare una connessione, logica o fisica, a un dispositivo o a una rete, rilevante ai fini della valutazione del rischio di *cybersecurity*. Tali elementi, espressamente previsti dall'art. 2, par. 1, CRA, operano congiuntamente e delimitano il perimetro oggettivo di applicazione del Regolamento, fermo restando il sistema di esclusioni stabilito dai paragrafi 2, 3 e 4 del medesimo articolo, che sottrae specifiche categorie di prodotti alla disciplina. Tra le altre cose si consideri che, per applicare la procedura della conformità corretta, bisogna verificare se il prodotto sia classificato come sistema di IA ad alto rischio ai sensi dell'art. 6 AI Act e se esso appartenga alle categorie dei prodotti importanti o critici del CRA.

[68] Dal punto di vista tecnico, la vulnerabilità è intesa come una condizione di fragilità o una debolezza intrinseca di un sistema informativo, suscettibile di essere sfruttata da soggetti malevoli per comprometterne il funzionamento e, quindi, realizzare un attacco, generalmente al fine di trarne un indebito vantaggio. In termini non troppo dissimili l'art. 2, co. 1, lett. ii), d.lgs. 138/2024 (recepimento della NIS2), così come l'art. 2, n. 40), definisce la vulnerabilità descrivendola come «una debolezza, suscettibilità o difetto di prodotti, servizi o processi TIC che può essere sfruttato da una minaccia informatica». Per completezza, si riporta anche la definizione riportata all'art. 3, n. 16, DORA, che guarda la vulnerabilità rispetto all'ambito finanziario specificando che si tratta di «*a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited*».

[69] L'intelligenza artificiale, prodotti con elementi digitali e l'Internet of Things (IoT) emergono come tecnologie capaci di amplificare le vulnerabilità dell'ecosistema *cyber*, estendendo la superficie di attacco e aumentando la complessità dei sistemi esposti: ogni dispositivo connesso funge da potenziale punto di ingresso per cyberattacchi spesso a causa di vulnerabilità tecniche, mancanza degli aggiornamenti o misure di sicurezza deboli.

[70] Artt. 6 e 7 CRA: rispettivamente rubricati "Requisiti per i prodotti con elementi digitali" e "Prodotti con elementi digitali critici". Cfr. Allegato I, parte I relativo ai Requisiti di cibersicurezza relativi alle proprietà dei prodotti con elementi digitali.

Pur configurando il rischio come una caratteristica intrinseca[71] del prodotto digitale, il CRA impone ai fabbricanti di governarlo sin dalla fase di progettazione e lungo l'intero ciclo di vita, mediante un approccio *risk-based*. Esso si traduce, in particolare, in obblighi di valutazione del rischio[72] fondati su parametri giuridicamente rilevanti quali la finalità prevista, l'uso ragionevolmente prevedibile[73] (incluso l'uso improprio ipotizzabile)[74] e la durata attesa del prodotto. Si tratta di elementi espressamente richiamati dall'interpretazione fornita dalla Commissione.[75] Specularmente, il regolamento mira a garantire che utenti e consumatori siano adeguatamente informati sugli *standard* di sicurezza del prodotto sin dal momento dell'acquisto, consentendo loro di poter fare affidamento su prodotti digitali conformi, certificati[76], aggiornati,[77] e, pertanto, in questo senso, *cybersafe*.
L'obbligo generale principale per i fabbricanti è quello di conformarsi ai

[71] R. Leszczyna, *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*, Cham, 2019, 149 ss.

[72] Ai sensi dell'art. 13 CRA, rubricato "Obblighi dei fabbricanti", il fabbricante è tenuto a effettuare una valutazione dei rischi *cyber* che deve essere presa in considerazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto. Se il fabbricante integra componenti di terze parti, deve esercitare la dovuta diligenza in modo che tali componenti non compromettano la *cybersecurity* del suo prodotto con elementi digitali. La valutazione del rischio, nonché i mezzi che il fabbricante sceglie per attuare i requisiti essenziali (ad esempio, norme o altre misure tecniche), devono essere inclusi nella documentazione tecnica. Il fabbricante è tenuto a tenere la documentazione a disposizione delle autorità di vigilanza del mercato, in quanto possono richiederla nell'ambito delle loro attività di applicazione.

[73] Ovvero un uso che è probabile possa derivare da un comportamento umano o da operazioni o interazioni tecniche ragionevolmente prevedibili, come previsto dall'art. 2, n. 24), CRA.

[74] L'art. 2, n. 25), CRA lo definisce come «l'uso di un prodotto con elementi digitali in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi ragionevolmente prevedibili».

[75] Commissione Europea, *FAQs on the Cyber Resilience Act*, in *digital-strategy.ec.europa.eu*, 3 dicembre 2025.

[76] Prima dell'immissione sul mercato di un prodotto con elementi digitali, il fabbricante è tenuto a svolgere la procedura di valutazione della conformità prescelta (*conformity assessment*), secondo quanto previsto dal capo III del regolamento. Qualora tale procedura abbia esito positivo, il fabbricante redige la dichiarazione UE di conformità, attestando così il rispetto dei requisiti essenziali di *cybersecurity* applicabili, come definiti nell'allegato I e richiamati, in particolare, dagli artt. 27 e 28 del regolamento, e appone la marcatura CE sul prodotto (artt. 29 e 30).

[77] Il fabbricante deve stabilire un periodo di supporto per il suo prodotto con elementi digitali, durante il quale garantirà che le vulnerabilità di tale prodotto siano gestite in modo efficace, in linea con i requisiti di gestione delle vulnerabilità (cfr. allegato I). La data di fine del periodo di supporto (compresi mese e anno) deve essere chiaramente e comprensibilmente specificata al momento dell'acquisto.

requisiti essenziali di *cybersecurity* di cui all'Allegato I, parte I (cfr. art. 13, par. 1),[78] nonché di implementare processi strutturati di *vulnerability assestment*,[79] divulgazione coordinata delle vulnerabilità e rilascio di aggiornamenti di sicurezza lungo l'intero ciclo di vita del prodotto (Requisiti di processo allegato I, parte II),[80] ai quali si aggiungono obblighi specifici di segnalazione (delle vulnerabilità, degli incidenti e dei quasi-incidenti) al CSIRT competente.[81] Nella prospettiva del CRA, la vulnerabilità non si

[78] L'art. 13 CRA stabilisce che i fabbricanti, al momento dell'immissione sul mercato, devono garantire che i prodotti con elementi digitali siano progettati, sviluppati e realizzati in conformità ai requisiti essenziali di *cybersecurity* di cui all'allegato I. A tal fine, essi sono tenuti a svolgere una valutazione dei rischi *cyber*, i cui risultati devono essere integrati lungo l'intero ciclo di vita del prodotto - dalla pianificazione alla manutenzione - al fine di ridurre i rischi, prevenire gli incidenti e limitarne l'impatto, anche in relazione alla salute e alla sicurezza degli utilizzatori.

[79] Il sistema di valutazione si articola secondo un approccio graduato, proporzionato al livello di rischio associato al prodotto. In linea generale, il fabbricante può ricorrere a procedure di autocertificazione o valutazione da parte di terzi; tuttavia, per determinate categorie di prodotti (prodotti importanti e critici elencati rispettivamente nell'allegato III e nell'allegato IV) considerati rilevanti sotto il profilo della *cybersecurity* quali, ad esempio, *software* di sicurezza, sistemi di gestione delle reti o componenti critici del sistema, è richiesto il rispetto di norme armonizzate oppure l'intervento di un organismo notificato, ossia un soggetto terzo incaricato della valutazione indipendente della conformità. Inoltre, per specifiche categorie di prodotti ritenuti particolarmente critici, tra cui taluni componenti destinati a garantire funzioni di sicurezza avanzate (quali *firewall*, elementi di sicurezza o *hypervisor*), il ricorso alla valutazione da parte di terzi assume carattere obbligatorio (art. 32 e allegato VIII). Tale articolazione riflette la logica del CRA, che combina un approccio *risk-based* con meccanismi differenziati di verifica della conformità, al fine di garantire un elevato livello di sicurezza dei prodotti digitali immessi nel mercato.

[80] Inoltre, assieme al prodotto con elementi digitali, deve fornire anche specifiche informazioni. L'art. 13 e l'Allegato II CRA definiscono un set minimo di informazioni e istruzioni rivolte all'utilizzatore che il fabbricante accompagna ai prodotti con elementi digitali, tra cui: dati identificativi e contatti del fabbricante, punto di contatto per la segnalazione delle vulnerabilità e politica di *disclosure*, caratteristiche e finalità del prodotto, proprietà di sicurezza e rischi prevedibili, durata del supporto e aggiornamenti di sicurezza, nonché istruzioni per l'uso sicuro, l'installazione degli aggiornamenti, la gestione del fine vita e, ove applicabile, l'integrazione in altri sistemi.

[81] Gli obblighi di segnalazione sono obbligatori ai sensi dell'art. 14 CRA. L'articolo in parola prevede che, una volta immesso il prodotto sul mercato, il fabbricante è tenuto a notificare le vulnerabilità sfruttate attivamente e gli incidenti gravi che hanno un impatto sulla sicurezza del prodotto di cui esso viene a conoscenza. In caso di incidente, il fabbricante deve notificare al CSIRT dello Stato membro in cui ha lo stabilimento principale e all'ENISA (entro 24 ore con una rapida segnalazione ed entro 72 ore con una notifica, oltre a successive relazioni da effettuarsi anche a seconda della gravità), mediante una piattaforma unica di comunicazione istituita e gestita dall'ENISA che sarà pienamente operativa da settembre 2026. Il CSIRT ricevente diffonderà la notifica ai CSIRT di altri Stati membri sul cui territorio è presente il prodotto in questione. Gli obblighi di comunicazione si applicano già a tutti i prodotti digitali che sono stati immessi sul mercato UE, dunque anche prima dell'11 dicembre 2027. Inoltre, il successivo art. 15 CRA prevede

configura come un mero fattore eventuale di rischio: la sua gestione non è completamente rimessa alla valutazione del soggetto obbligato, come piuttosto avviene nel sistema di gestione delle vulnerabilità previsto dalla NIS2.[82] La vulnerabilità è un elemento strutturale e intrinseco del prodotto digitale, che deve essere identificato, monitorato e gestito in modo continuo e autonomo rispetto ad altri fattori di rischio, secondo la logica proattiva[83] e proceduralizzata del CRA. Questa impostazione riflette una più ampia evoluzione della *governance* europea della *cybersecurity*, che si sposta da un paradigma centrato sulla resilienza tecnico-organizzativa - tipico delle infrastrutture e dei servizi essenziali - a un modello orientato alla security by design, nel quale la *compliance* è incorporata nella stessa architettura tecnica dei prodotti.[84]

Sebbene, in linea teorica, ogni processo di gestione del rischio dovrebbe muovere dall'identificazione delle vulnerabilità, nel CRA emerge un approccio che può definirsi "atomistico", in quanto incentrato sul singolo prodotto con elementi digitali, in contrapposizione alla logica sistemica propria della normativa NIS2 e, come si dirà, del PSNC.

Il CRA, infatti, disciplina la sicurezza a livello di prodotto, imponendo che ciascun elemento *hardware* o *software* sia progettato, sviluppato e mantenuto aggiornato in modo tale da gestire le proprie vulnerabilità lungo l'intero ciclo di vita, conformemente ai requisiti essenziali di *cybersecurity* e ai processi di *vulnerability handling* previsti dal regolamento.[85] Tuttavia, tale impostazione presuppone un'interazione con la dimensione sistemica: qualora il prodotto digitale o le sue componenti siano utilizzati all'interno di un soggetto rientrante nell'ambito della NIS2 o in contesti critici, anche nazionali - come i soggetti PSNC - essi divengono parte integrante del sistema organizzativo e, come tale, possono rilevare ai fini della gestione del rischio complessivo. Le vulnerabilità del singolo prodotto, pertanto, vengono riportate al contesto in cui esso è inserito.

In questa prospettiva, vulnerabilità e minacce informatiche non restano confinate alla dimensione tecnica, ma si proiettano nel sistema-organiz-

anche le segnalazioni volontarie che possono essere fatte da qualsiasi persona fisica o giuridica notificando le vulnerabilità, le minacce informatiche, gli incidenti e i quasi incidenti attraverso la suddetta piattaforma unica di comunicazione. Si veda Commissione Europea, *Legge sulla ciberresilienza - Sintesi del testo legislativo*, in *digital-strategy.ec.europa.eu*, 3 dicembre 2025.

[82] Art. 21 NIS2 trasposto nell'art. 24, c. 2, lett. e), Decreto NIS2.

[83] J. Ruohonen-P. Timmers, *Vulnerability coordination under the Cyber Resilience Act*, in *Applied Cybersecurity & Internet Governance*, 2025.

[84] ENISA, *Coordinated Vulnerability Disclosure Policies in the EU*, in *enisa.europa.eu*, aprile 2022.

[85] J. Ruohonen-P. Timmers, *Vulnerability coordination under the cyber resilience act*, in Applied Cybersecurity & Internet Governance, 4(1), 2025.

zazione, contribuendo a determinarne il livello di esposizione al rischio e attivando, conseguentemente, i relativi obblighi di gestione previsti dalle normative di riferimento. Il CRA è destinato a configurarsi come un punto di riferimento per i prodotti digitali "a marchio CE"[86] - analogamente al ruolo svolto dal GDPR nell'ambito della protezione dei dati personali contribuendo alla progressiva standardizzazione europea dei requisiti di sicurezza digitale[87] e minimizzazione di rischi nel mercato interno.[88] La mancata conformità ai requisiti essenziali di *cybersecurity* e agli ulteriori obblighi previsti dal CRA può comportare, infatti, sanzioni pecuniarie significative, limitazioni o divieti di commercializzazione del prodotto, nonché potenziali forme di responsabilità, rafforzando la natura cogente della disciplina.[89]

Nel contesto nazionale, il quadro della gestione del rischio *cyber* è ulteriormente rafforzato dal Perimetro di Sicurezza Nazionale Cibernetica (PSNC), istituito dal d.l. 105/2019 (Decreto Perimetro), convertito con modificazioni dalla l. 133/2019 (Legge Perimetro), con l'obiettivo di assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi ICT[90] delle amministrazioni pubbliche e degli operatori pubblici e privati che svolgono funzioni essenziali o erogano servizi essenziali per lo Stato. In particolare, il Perimetro si applica ai soggetti da cui dipende l'esercizio di funzioni fondamentali dello Stato o la prestazione di servizi essenziali per il mantenimento di attività civili, sociali ed economiche di rilevanza strategica, il cui malfunzionamento, interruzione o uso im-

[86] La Commissione Europea ha specificato che i prodotti interessati recheranno la marcatura CE per indicare la conformità *cyber* ai requisiti del CRA, mentre le autorità nazionali di vigilanza del mercato garantiranno l'applicazione delle relative disposizioni. In generale, il "marchio CE" compare già su molti prodotti commercializzati nel mercato unico esteso dello Spazio Economico Europeo ed indica che sono stati valutati come conformi a elevati requisiti di sicurezza, salute e tutela dell'ambiente. Si veda Commissione Europea, *Cyber Resilience Act,* in *digital-strategy.ec.europa.eu*, 3 dicembre 2025.

[87] I. Kamara, *Standardizing personal data protection*, Oxford, 2025; 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*, 37(5), 2024, 1441 ss.

[88] P. Car-S. De Luca, *EU Cyber resilience act*, European Parliament Research Service, in *europarl.europa.eu*, dicembre 2024.

[89] Per una panoramica più approfondita della disciplina del CRA, anche in merito ai requisiti orizzontali di *cybersecurity*, si rimanda a F. Teichmann-B.S. Sergi, *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in *Computer Law & Security Review*, 59, 2025; P.G. Chiara, *Understanding the regulatory approach of the Cyber Resilience Act: protection of fundamental rights in disguise?*, in *European Journal of Risk Regulation*, 16(2), 2025, 469 ss.

[90] Ai sensi dell'art. 1, lett. l), D.P.C.M. 131/2020 il "Servizio informatico" è «un servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi informativi, ivi incluso quello di cloud computing».

proprio possa comportare un pregiudizio per la sicurezza nazionale (art. 1, c. 1 e 2, Decreto Perimetro). I soggetti inclusi nel PSNC, individuati mediante criteri e procedure stabiliti dal D.P.C.M. 131/2020,[91] operano in settori strategici quali interno, difesa, energia, telecomunicazioni, trasporti, economia e finanza, spazio e aerospazio, tecnologie critiche e servizi digitali, enti previdenziali e del lavoro (art. 3, c. 1), e sono tenuti a predisporre e aggiornare periodicamente un inventario dettagliato delle reti, dei sistemi informativi e dei servizi ICT di propria pertinenza - come previsto dall'art.1, c. 2, lett. b), Decreto Perimetro[92] - comprensivo della relativa architettura e componentistica.[93] Tali elenchi assumono un ruolo centrale nella gestione del rischio, in quanto consentono l'identificazione degli *asset* critici da cui dipendono funzioni e servizi essenziali, nonché la valutazione delle vulnerabilità suscettibili di incidere sulla sicurezza nazionale. Tale obbligo si inserisce in una logica di gestione del rischio fondata sull'identificazione degli *asset* critici da cui dipendono funzioni e servizi essenziali e sulla valutazione delle possibili conseguenze derivanti da mal-

[91] Un soggetto è qualificato come rilevante, ai sensi dell'art. 2, c. 1, lett. a) e b), D.P.C.M. 131/2020, quando esercita una funzione essenziale dello Stato o fornisce un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali. Nel primo caso, si tratta di soggetti ai quali l'ordinamento attribuisce compiti volti a garantire la continuità dell'azione di Governo e degli organi costituzionali, nonché la tutela della sicurezza interna ed esterna, della difesa dello Stato, delle relazioni internazionali, dell'ordine e della sicurezza pubblica, dell'amministrazione della giustizia e del corretto funzionamento dei sistemi economico-finanziari e dei trasporti. Nel secondo caso, rientrano invece i soggetti che svolgono attività strumentali all'esercizio di tali funzioni, attività necessarie per l'esercizio e il godimento dei diritti fondamentali, per la continuità delle forniture e l'efficienza delle infrastrutture e della logistica, nonché attività di ricerca e produzione, in particolare nei settori ad alta tecnologia o in altri ambiti di rilevanza economica e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico . Tale duplice qualificazione assume rilievo centrale nella prospettiva della gestione del rischio, in quanto individua i soggetti la cui esposizione a vulnerabilità può tradursi in un impatto sistemico e, in ultima istanza, in un pregiudizio per la sicurezza nazionale. L'elenco dei soggetti inclusi è stato adottato con atto amministrativo del Presidente del Consiglio dei ministri, su proposta del Comitato Interministeriale per la Cybersicurezza. L'elenco viene aggiornato, ma non è soggetto a pubblicazione ed è sottratto al diritto di accesso, fermo restando l'obbligo di comunicazione individuale ai soggetti interessati.

[92] Il riferimento all'art. 1, c. 2, lett. b), Decreto Perimetro trova attuazione nell'art. 7 D.P.C.M. 131/2020, che disciplina i criteri e le modalità procedurali per la predisposizione e l'aggiornamento di tali elenchi.

[93] Per "Architettura e componentistica" l'art. 1, lett. n), D.P.C.M. 131/2020 intende «l'insieme delle architetture realizzate e dei componenti usati a livello di rete, dati e software, ivi inclusi la distribuzione su piattaforme di cloud computing, nonché le procedure e i flussi informativi per l'accesso, acquisizione, trasmissione, conservazione, elaborazione e recupero dei dati necessari all'espletamento dei servizi informatici».

funzionamenti o compromissioni.[94] In questo quadro, il PSNC introduce obblighi specifici di sicurezza e di notifica degli incidenti al CSIRT Italia,[95] nonché l'adozione di misure tecniche e organizzative volte a garantire un elevato livello di protezione, in linea con gli *standard* europei e internazionali. Tra questi, i soggetti Perimetro sono tenuti a permettere di effettuare uno «screening tecnologico degli approvvigionamenti ICT appartenenti a categorie specifiche destinati ai beni ICT perimetro».[96] Si tratta, di fatto, di un obbligo di notifica preventiva in relazione alle procedure di approvvigionamento di beni, sistemi e servizi ICT destinati a essere impiegati su *asset* strategici rientranti in specifiche categorie individuate dalla normativa di attuazione. In particolare, i soggetti devono comunicare al Centro di Valutazione e Certificazione Nazionale (CVCN) l'intenzione di procedere all'affidamento, anche per il tramite di centrali di committenza, di forniture relative a beni, sistemi e servizi ICT rientranti nelle categorie individuate dal D.P.C.M. 15 giugno 2021, prima dell'avvio della procedura di gara o della conclusione del contratto.

Il CVCN, istituito presso l'ACN, ha, infatti, il compito di valutare preventivamente la sicurezza dei beni, sistemi e servizi ICT destinati ad essere impiegati nel Perimetro, verificando, in particolare, le caratteristiche di *security by design* e l'assenza di vulnerabilità note.[97] Tale obbligo si inserisce in una

[94] Nel PSNC la nozione di pregiudizio per la sicurezza nazionale è intesa come danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche che ne costituiscono il fondamento, nonché agli interessi politici, militari, economici, scientifici e industriali dello Stato, derivante dall'interruzione o dalla compromissione di una funzione essenziale o di un servizio essenziale. A tal fine, il concetto di compromissione è definito dall'art. 1, lett. f) e g), D.P.C.M. 131/2020 come la perdita di sicurezza o di efficacia nello svolgimento di tali funzioni o servizi, connessa al malfunzionamento, all'interruzione, anche parziale, o all'uso improprio di reti, sistemi informativi e servizi ICT. Tale definizione risulta particolarmente rilevante nella prospettiva della gestione del rischio *cyber*, in quanto esplicitano il nesso tra vulnerabilità tecnica, compromissione operativa e danno sistemico, contribuendo a qualificare il rischio non solo in termini economici-probabilistici, ma anche in relazione al suo impatto sugli interessi fondamentali dello Stato e sul prestigio della funzione pubblica.

[95] Per una panoramica in materia si rimanda a S. Mele, *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. Cassano–S. Previti (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, 186.

[96] Per ulteriori chiarimenti e per l'evoluzione delle *policy* e della normativa *cyber* nazionale si veda Senato della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza* (riferita al 2020), Doc. XXXIII n. 3, 97 ss.

[97] Il CVCN definisce, inoltre, metodologie di test e verifica, contribuisce alla definizione delle misure di sicurezza e può imporre condizioni e prescrizioni specifiche per l'utilizzo dei prodotti, anche avvalendosi di laboratori accreditati. Si noti che si tratta di procedure complesse, anche composta da varie fasi di *assesment* del rischio *cyber* e delle vulnerabilità, per la quale si rimanda al D.P.R. 54/2021.

logica di gestione proattiva del rischio, consentendo al CVCN di effettuare valutazioni preliminari in ordine alla sicurezza delle soluzioni tecnologiche proposte, con particolare riferimento alla presenza di vulnerabilità e alla loro idoneità rispetto al contesto di impiego. In questo senso, la fase di *procurement* diviene un momento importante di controllo del rischio *cyber*, in cui la sicurezza dei prodotti e dei servizi ICT è verificata *ex ante*, contribuendo a prevenire l'introduzione di elementi vulnerabili all'interno di infrastrutture strategiche che possono annidarsi nelle *supply chain*.

Il PSNC, a livello domestico, è uno strumento di rafforzamento della sicurezza nazionale che integra, e in parte amplia, l'ambito applicativo della normativa unionale, includendo anche soggetti, prodotti e processi che non rientrano necessariamente nella sua disciplina. In molti casi, tuttavia, i soggetti NIS2 coincidono con quelli del Perimetro - nonché con quelli della l. 90/2024 - determinando una sovrapposizione funzionale tra i due regimi, soprattutto in relazione agli obblighi di gestione del rischio e di notifica degli incidenti al CSIRT Italia. Se la NIS2 opera sul piano della resilienza infrastrutturale e il CRA su quello della sicurezza del prodotto, il Perimetro introduce una dimensione strategico-nazionale, in cui la gestione del rischio è orientata alla tutela della sicurezza dello Stato. In tale prospettiva, emerge chiaramente come il prodotto digitale diventi un elemento critico anche all'interno dei sistemi inclusi nel PSNC: le fragilità *cyber* del singolo prodotto, infatti, possono mettere a rischio la sicurezza nazionale, confermando la centralità di un approccio integrato e proattivo alla *cybersecurity*, fondato sulla formazione, sulla valutazione continua del rischio e sulla gestione strutturata delle vulnerabilità. La *cybersecurity law* si inserisce, di conseguenza, in modo sempre più coerente e trasversale nel più ampio ecosistema normativo europeo e nazionale del digitale, contribuendo a completarlo, a rafforzare le discipline esistenti e ad assumere un ruolo progressivamente centrale, favorendo un'integrazione sistemica.

In particolare, il CRA si coordina direttamente con la regolazione dell'intelligenza artificiale, come emerge dall'art. 12, che prevede espressamente una presunzione di conformità dei prodotti digitali che sono anche sistemi di IA ad alto rischio ai sensi dell'AI Act. Attraverso tale disposizione, il legislatore europeo realizza un coordinamento che consente di integrare i requisiti di *cybersecurity* del CRA all'interno del più ampio *framework* di gestione del rischio dei sistemi di IA, confermando il ruolo del prodotto digitale quale nuovo *standard* tecnico[98] su cui si innestano i sistemi complessi. Ne deriva, pertanto, un modello regolatorio integrato e multilivello, in cui la sicurezza dei prodotti (ai sensi del CRA, che tutela altresì la protezione dei dati personali), la resilienza dei sistemi e dei servizi critici (ai sensi della

[98] Per maggiori chiarimenti, si veda I. Kamara-M. Bassini, *The cybersecurity and AI nexus in the EU digital acquis*, in questa *Rivista*, 1, 2025, 312 ss.

NIS2 e della normativa *cyber* nazionale) e la gestione del rischio nei sistemi di intelligenza artificiale (ai sensi dell'AI Act) operano in modo coordinato e interdipendente. Se il CRA stabilisce quali prodotti digitali sono tecnicamente conformi agli *standard* UE, la normativa in materia di intelligenza artificiale si concentra sui rischi per i diritti fondamentali e la sicurezza derivanti dall'uso di tali sistemi. L'AI Act organizza il quadro regolatorio secondo una struttura piramidale articolata in quattro livelli (inaccettabile, ad alto rischio, a rischio limitato e a rischio minimo), modulando gli obblighi in funzione della gravità del rischio connesso all'uso del sistema di AI e alle sue potenziali conseguenze. Il legislatore unionale ha ritenuto di dover vietare determinate pratiche inaccettabili, mentre ha stabilito requisiti specifici per i sistemi ad alto rischio (tra i quali quello di *cybersecurity*) e obblighi per gli operatori (cfr. considerando 26 AI Act). I principi di proporzionalità e trasparenza, coniugati con l'approccio basato sul rischio, garantiscono la tutela dei diritti fondamentali, senza ostacolare indebitamente i benefici che l'innovazione tecnologica può offrire.[99]

Sebbene sia la *cybersecurity* che l'AI adottino un paradigma regolatorio "*risk-based*", le modalità concrete di applicazione divergono: i sistemi di gestione del rischio consentono di tradurre in obblighi operativi un rischio che, a seconda delle finalità, dell'assetto decisionale del legislatore e della natura del rischio, può presentarsi come più o meno identificato.[100] In questo senso è fondamentale distinguere tra rischi e incertezze. Alcuni studiosi definiscono i rischi come "*known knowns*", ovvero eventi prevedibili per i quali è possibile stimare probabilità e impatti; le incertezze sono invece "*known unknowns*", situazioni note come ignote, non quantificabili, in quanto gli effetti di una specifica tecnologia non sono attualmente prevedibili. Vi è poi la dimensione degli "*unknown unknowns*", fenomeni dai quali non si sospettano, allo stato, neppure le possibili conseguenze avverse.[101]

Nel contesto della normativa *cyber* del macro-filone strategico (NIS2, CER, DORA), la responsabilità dell'identificazione e della valutazione del rischio è attribuita direttamente ai soggetti obbligati. Le organizzazioni, in quanto esperte del proprio assetto e contesto, sono chiamate a selezionare, prioritizzare e gestire i rischi in funzione della probabilità e dell'impatto. Nel CRA, questa libertà decisionale risulta notevolmente attenuata.[102]

---

[99] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, in *European Journal of Risk Regulation*, 16(2), 2025, 684 ss.

[100] A. Gullo, *Compliance*, cit., 1 ss.

[101] J. Black., *The role of risk in regulatory processes*, in R. Baldwin-M. Cave-M. Lodge (a cura di), *The Oxford Handbook of Regulation*, Oxford, 2010, 302 ss. e 310. Così anche M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[102] F. Teichmann-B.S. Sergi, *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in *Computer Law & Security Review*, 59, 2025,

Nell'AI Act, invece, per ogni sistema di AI ad alto rischio, il fornitore deve prevedere un sistema di gestione dei rischi che operi in modo «iterativo, pianificato e continuo» per l'intero ciclo di vita del sistema (dalla progettazione, allo sviluppo, al rilascio, all'aggiornamento e al ritiro), che tenga conto della finalità e del contesto dello stesso. Tale processo ha la finalità di identificare, stimare, valutare e mitigare non solo i rischi noti relativi all'uso conforme alla finalità prevista, ma anche i rischi derivanti da usi «impropri ragionevolmente prevedibili», ossia scenari conseguenti a comportamenti umani prevedibili in contesti reali.[103] In altre parole, questo vuol dire prevedere attaccanti o eventi *cyber* che possano usare il sistema di AI per scopi diversi o in modo errato, sebbene non esplicitato dalla normativa. Le decisioni del fornitore su quali misure di mitigazione adottare per i sistemi di AI ad alto rischio, e in quali casi accettare un rischio residuo, devono essere giustificate, documentate e, se appropriato, basate sul coinvolgimento di esperti o *stakeholder* esterni. Differentemente, il sistema di gestione del rischio previsto nella NIS2 tende alla verticalizzazione all'interno dell'organizzazione obbligata.

Le istruzioni per l'uso fornite dal fornitore di sistemi di AI ad alto rischio devono includere gli scenari di utilizzo improprio prevedibile, in modo che il *deployer* sia consapevole dei rischi potenziali. La normativa *cyber*, invece, prevede formazione del personale dell'organizzazione e l'aggiornamento continuo della sicurezza dei prodotti digitali. Le misure di mitigazione attuate nel contesto dell'AI Act devono riflettere lo stato dell'arte (normativo e tecnologico) e, in caso di rischi residui, non è richiesto che il fornitore eroghi formazione all'utenza o preveda addestramenti aggiuntivi al sistema stesso, benché tali accorgimenti siano incoraggiati, quando utili, per attenuare gli usi impropri ragionevolmente prevedibili. Il sistema di gestione dei rischi dei sistemi di AI ad alto rischio deve essere periodicamente riesaminato e aggiornato per garantirne costantemente l'efficacia, e ogni scelta significativa nel processo deve essere documentata, così da poter dimostrare conformità alle autorità regolatorie. I soggetti obbligati ai sensi dell'AI Act, dunque, non sono esenti da una valutazione del rischio: al contrario, essi devono effettuare una più complessa analisi di impatto[104] per tutti quei sistemi che potrebbero portare a lesioni dei diritti fondamentali e discriminazioni derivanti da decisioni automatizzate.[105]

A differenza del rischio *cyber*, di derivazione principalmente tecnocentrica,

106209 ss.

[103] Cfr. consideranda 64 e 65 e art. 9 AI Act.

[104] *Ibid.*

[105] O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali,* 43(3), 2023, 569 ss.; O. Pollicino-P. Dunn, P., *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*, Milano, 2024.

quello preso in considerazione in materia di AI è un rischio di derivazione antropocentrica. Nella normativa sulla *cybersecurity* l'attenzione è rivolta, tra l'altro, a vulnerabilità, attacchi all'integrità delle catene di fornitura, ai difetti infrastrutturali o dei sistemi, processi e prodotti ICT, alla difesa e resilienza delle componenti logiche e fisiche dei sistemi informativi e delle reti. Il legislatore interviene imponendo misure di sicurezza, obblighi di aggiornamento, *standard* tecnici, certificazioni e notifiche obbligatorie. Nel corso dei negoziati sull'AI Act, il legislatore europeo si è confrontato con la complessa individuazione dei criteri idonei a determinare quando un sistema di intelligenza artificiale possa essere considerato portatore di un rischio inaccettabile per gli individui, nonché con la definizione delle pratiche da vietare e delle categorie di sistemi da qualificare come "ad alto rischio" per la società, ammissibili solo a determinate condizioni. In tale contesto, è emersa una criticità degli approcci basati sul rischio, consistente nella difficoltà di raggiungere un consenso condiviso sia sull'individuazione dei rischi rilevanti sia sulla loro graduazione in termini di gravità. Questo processo ha alimentato un ampio dibattito a livello europeo, evidenziando le sfide connesse alla regolazione di una tecnologia in rapida evoluzione, ancora caratterizzata da limitate evidenze empiriche circa i suoi impatti sociali.[106]
L'AI Act e la Legge AI nazionale non lasciano il compito di valutare i punteggi di rischio ai soggetti obbligati, ma identificano e classificano direttamente le diverse categorie di rischio in modalità "*top-down*".[107]

2.1 Modalità di valutazione del rischio della normativa cyber e di intelligenza artificiale

La gestione del rischio *cyber* non riguarda la sola gestione del rischio tecnico. Nel 2025, il 95% degli attacchi *ransomware* ha colpito soggetti privi di particolari obblighi normativi o appartenenti a settori considerati a minore criticità, mentre solo il 5% ha interessato operatori soggetti a regimi normativi specifici.[108] Da questi dati si evince l'importanza della normativa *cyber*, che prevede un sistema di gestione adattabile al contesto, anche per quelle organizzazioni che, pur non essendo obbligate alla *compliance* normativa NIS2, e tantomeno al CRA o al PSNC, possono trovare nella *cybersecurity law* un sistema consolidato e integrato, basato sull'analisi com-

[106] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[107] G. De Gregorio-P. Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, cit.

[108] Quali il PSNC, la NIS, la normativa Telco, la l. 90/2024, il DORA e il CRA.

plessiva del rischio informatico.[109]
Per mitigare il rischio di compromissione dei sistemi informativi e di rete, la normativa NIS2 prevede un modello di gestione del rischio con obblighi di sicurezza calibrati sul livello di rischio effettivo al quale ciascun soggetto è esposto.[110] In particolare, il decreto NIS2 impone a soggetti essenziali e importanti[111] - individuati sulla base degli Allegati I-IV - di adottare misure tecniche, operative e organizzative adeguate e proporzionate per garantire la sicurezza delle reti e dei sistemi informativi utilizzati nello svolgimento delle proprie attività o nella fornitura dei loro servizi per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per gli altri.[112]
Tale obbligo risponde, ai sensi dell'art. 24, c. 1, decreto NIS2, a due principi: (*i*) il principio di adeguatezza, che richiede di considerare le «conoscenze più aggiornate e lo stato dell'arte» nell'individuazione delle misure di sicurezza - dunque tecnologie, normative e *standard* di riferimento[113] e (*ii*) il principio di proporzionalità, che impone alle organizzazioni di calibrare le misure «al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico».
La normativa impone, inoltre, precisi obblighi di comunicazione in caso di incidente significativo:[114] una pre-notifica al CSIRT Italia[115] entro 24 ore dalla conoscenza dell'evento, una notifica completa entro 72 ore, e la trasmissione di una relazione finale dettagliata che descriva causa, impatto e misure adottate (art. 25, Decreto NIS2). Tale valutazione si inserisce in una più ampia funzione di responsabilizzazione dei vertici e della *governance* dell'organizzazione (art. 23, Decreto NIS2), che sono chiamati non solo a deliberare l'adozione delle misure di gestione del rischio, ma anche a sorvegliare sull'attuazione e sul continuo aggiornamento delle stesse, raf-

[109] Si veda ACN, *Operational Summary del 1° semestre 2025*, cit.

[110] *Ibid.*

[111] La normativa si applica a diciotto settori critici suddivisi in due categorie: undici settori essenziali e sette settori importanti.

[112] Art. 24 d.lgs. 138/2024.

[113] *Ibid.*

[114] Per la normativa NIS2 deve trattarsi di incidenti significativi. Ai sensi dell'art. 25, c. 4, Decreto NIS2 un incidente è considerato significativo se: (*i*) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; (*ii*) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

[115] Il CSIRT Italia, in caso di incidenti *cyber* o notifiche di eventi, è l'interlocutore unico per tutti i soggetti pubblici e privati in quanto destinatario delle notifiche obbligatorie e segnalazioni volontarie previste dalla normativa *cyber*.

forzando così l'efficacia complessiva della sicurezza informatica dell'organizzazione.

La possibilità che le minacce informatiche[116] divengano incidenti si verifica quando viene sfruttata con successo una vulnerabilità dell'organizzazione. In un contesto di dipendenza dalle reti e sistemi informativi, eventi quali «l'accesso non autorizzato ai dati, la loro divulgazione senza consenso, la manipolazione o la distruzione costituiscono minacce concrete in grado di produrre conseguenze dannose non solo per la singola organizzazione, ma per l'intera società e l'economia del Paese, ad esempio in caso di blocco di servizi critici».[117]

Il rischio è «la combinazione dell'entità dell'impatto di un incidente[118], in termini di danno o di perturbazione, e della probabilità che esso si verifichi» (decreto NIS2).[119] In altre parole, è definito «dall'impatto della minaccia su un determinato bene, persona o valore, tenuto conto del grado della probabilità che tale evento si verifichi»:[120] una definizione, questa, riportata in termini analoghi dall'art. 3, par. 2, AI Act.

La formula concettuale Rischio = Probabilità × Impatto è coerente anche ai più comuni *standard* internazionali di settore quali la ISO e il *framework* NIST ed è un'utile formulazione del concetto ai sensi della normativa *cyber* e di AI nazionale ed unionale. Resta, tuttavia, un punto di partenza: la formula, infatti, deve essere letta in senso dinamico, potendo integrare pesi, fattori correttivi e ponderazioni che riflettano la specificità, ad esempio, del contesto organizzativo, della natura dei servizi e del livello di esposizione alle minacce.

A livello operativo, l'art. 24 Decreto NIS2 richiede che le misure di sicurezza siano adattate a fattori tecnologici (livello di interconnessione, dipendenze infrastrutturali), organizzativi (dimensioni, natura dei servizi

---

[116] Art. 2, lett. bb), d.lgs 138/ 2024, definizione di "minaccia informatica": «Qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone, così come definita dall'art. 2, punto 8), Regolamento (UE) 2019/881».

[117] ACN, *Domini della cybersicurezza - Event, Threat and Incident Management*, cit.

[118] Art. 2, par.1, lett. t), Decreto NIS. L'incidente è quell'«evento che compromette la disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi offerti o accessibili tramite reti e sistemi informativi» e che la *cybersecurity* vuole evitare.

[119] Similmente, ai sensi dell'art. 3, par. 37, Regolamento (UE) 2024/2847 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (CRA) il rischio *cyber* è «la potenziale perdita o perturbazione causata da un incidente da esprimersi come combinazione dell'entità di tale perdita o perturbazione e della probabilità che si verifichi l'incidente».

[120] M.A. Rizzi-F. Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 6(2), 2024, 115 ss.

erogati) ed economico-sociali (impatto potenziale sulla collettività e sulla sicurezza nazionale). Sono questi fattori di contesto a riempire di significato - e successivamente a rendere calcolabile - le due variabili della "probabilità" e dell'"impatto".

In attuazione dell'art. 31, c.1, Decreto NIS,[121] la Determinazione di ACN n. 164179/2025 ha fornito una mappatura delle misure di sicurezza di base[122] - oltre che di incidenti significativi - e le tempistiche per la loro applicazione, distinguendo tra requisiti di natura organizzativa (es. processi di *risk assessment*, procedure di gestione degli incidenti, ruoli) e requisiti tecnologici (es. strumenti di monitoraggio, cifratura, autenticazione multifattore), ribadendo che nella *cybersecurity* occorre un adattamento al contesto specifico del soggetto obbligato[123]. La prevalenza di misure per i soggetti essenziali rispetto a quelli importanti è coerente con il principio di proporzionalità della NIS2. Il maggior numero di misure organizzative rispetto a quelle tecniche, rispondono anche all'esigenza di efficienza e contenimento dei costi. Le misure di base identificate da ACN rispondono ad un obbligo, ma allo stesso tempo supportano le organizzazioni offrendo una prima interpretazione nella predisposizione degli elementi di gestione del rischio previsti dalla normativa, quali, ad esempio: (*i*) l'applicazione di politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete; (*ii*) le misure di gestione degli incidenti, incluse le notifiche agli organi competenti; (*iii*) i piani di continuità operativa e *disaster recovery*; (*iv*) i requisiti di sicurezza per la *supply chain* e per l'acquisizione, lo sviluppo e manutenzione dei sistemi; pratiche di sicurezza di base e formazione del personale[124]. Infatti, se da un lato questa normativa offre il vantaggio di non richiedere una modalità specifica per la loro applicazione, dall'altro può risultare complessa a quelle organizzazioni con un livello di *cyberculture* non ancora maturo.[125]

Il rischio *cyber* si distingue per la rapidità con cui può produrre effetti negativi su *asset* e persone, per la capacità di propagazione su scala globale e per l'elevato grado di interconnessione che ne amplifica la portata. A ciò

[121] La disposizione prescrive che ACN debba «stabilire obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico».

[122] Si veda *Framework Nazionale per la Cybersecurity e la Data Protection - Edizione 2025 (v2.1)*, in *cybersecurityframework.it*.

[123] ACN, *Modalità e specifiche di base*, in *acn.gov.it*.

[124] Art. 24, c. 2, d.lgs. 138/2024.

[125] M.A. Adamu-M.I. Niemimaa-P. Spagnoletti, *Towards a Three-Tiered Framework for Fostering Organizational Cybersecurity Culture*, in M. Themistocleous-N. Bakas-G. Kokosalakis-M. Papadaki (a cura di), *Information Systems. EMCIS 2024. Lecture Notes in Business Information Processing, vol 536*, Cham, 2025, 313 ss.

si aggiunge l'elemento intenzionale, rappresentato da attori malevoli che possono sfruttare le vulnerabilità tecniche, le persone, le reti e i sistemi informativi per finalità illecite.
In questo senso la dottrina[126] parla di un approccio al rischio *cyber* multidimensionale, dinamico ed integrato che deve essere parte della cultura organizzativa, che supera la logica della *compliance checklist* per orientarsi verso una vera e propria *risk governance* adattiva, in grado di coniugare obblighi giuridici e valutazioni tecnico-organizzative in un quadro di responsabilità condivisa tra operatori, Autorità di settore e ACN dove il contesto organizzativo è la chiave per comprendere i rischi ai quali va incontro l'organizzazione.
L'AI Act parte da una prospettiva differente. Il Regolamento in parola valuta i rischi connessi all'uso dell'AI e li categorizza per gravità: "inaccettabile" (e quindi pratiche vietate), "rischio alto", "rischio limitato" e "minimo o nullo".
L'art. 5 AI Act elenca i sistemi di AI[127] che devono essere eliminati dal mercato in quanto ritenuti una minaccia alla sicurezza, ai diritti fondamentali e alla vita delle persone ai sensi della Carta dei diritti fondamentali dell'UE. In particolare, sono vietati quei sistemi di AI che mirano a manipolare, discriminare o sorvegliare gli individui in modi sistematici. Tra questi rientrano quelli che usano tecniche subliminali o ingannevoli per alterare decisioni consapevoli degli individui; che sfruttano vulnerabilità personali - per età, disabilità, status socio-economico - per influenzarne il comportamento; che valutano o classificano le persone sulla base del loro comportamento sociale o della personalità, anche mediante riconoscimento facciale (identificazione biometrica remota in tempo reale) o sono capaci di riconoscere le emozioni nei luoghi di lavoro ecc.
Al secondo livello della piramide di rischio si trovano i sistemi di AI ad alto rischio. Questi sistemi vengono utilizzati in settori considerati critici che, per finalità o per il loro impatto sistemico, possono incidere significativamente sui diritti fondamentali, sulla sicurezza o sulla salute pubblica. È il caso, ad esempio, dei sistemi usati per la diagnosi medica o per la guida autonoma dei veicoli.
Prima di immettere un sistema di AI ad alto rischio sul mercato UE o di farlo entrare in servizio, i fornitori dovranno dimostrare che il loro sistema è affidabile e conforme ai requisiti richiesti per l'AI in relazione a qualità

[126] A. Gullo, *Compliance*, cit., 1 ss.

[127] Il sistema di intelligenza artificiale, ai sensi dell'art. 3, par. 1, AI Act, è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

dei dati, documentazione e tracciabilità, obblighi di trasparenza, sorveglianza umana in ogni fase critica, accuratezza, *cybersecurity* e robustezza dei sistemi.[128]
Inoltre, l'art. 9, rubricato "Sistema di gestione dei rischi", impone ai fornitori di sistemi AI ad alto rischio di condurre una valutazione d'impatto comprendente l'identificazione e l'analisi dei rischi prevedibili per salute, sicurezza o diritti fondamentali e, sulla base di tale valutazione, di istituire un sistema di gestione del rischio che accompagni il sistema per tutto il ciclo di vita, mediante misure mirate a mitigare i rischi identificati. Mentre la valutazione del rischio riguarda l'identificazione, l'analisi e la valutazione dei rischi legati all'AI, l'analisi d'impatto comprende conseguenze più ampie, ad esempio, su diversi *stakeholder* - utenti, società - e ambientali.[129]
Per quanto riguarda i sistemi di AI che presentano rischi ridotti, come *chatbot* o strumenti che generano contenuti, questi sono soggetti a obblighi di trasparenza: gli utenti devono essere informati che i contenuti (ad esempio, audio e video) sono prodotti con l'ausilio dell'AI, così da poterne fruire consapevolmente.[130] In definitiva, nel contesto dell'AI per i soggetti obbligati assume rilievo innanzitutto la soglia preventiva del rischio: la normativa classifica *ex ante* i sistemi di AI in fasce di rischio, al di là del calcolo sull'impatto del singolo contesto,[131] con obblighi, vincoli o divieti differenziati. È la classificazione normativa a stabilire a priori quale livello di rigore applicativo un sistema di AI debba rispettare indipendentemente da quanto ogni singolo operatore o sviluppatore ritenga che i rischi possano sussistere.

3. Le intersezioni dell'intelligenza artificiale con la *cybersecurity* a tutela dell'ecosistema *cyber*

L'interazione tra sistemi di AI con la *cybersecurity* è un rapporto virtuoso, ampiamente descritto dalla letteratura tecnica[132,133], nonché un interesse

[128] Si veda Dipartimento per il programma di Governo, *Analisi del quadro normativo in materia di Intelligenza artificiale (D.D.L. IA e Regolamento UE su IA)*, in *programmagoverno.gov.it*.

[129] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[130] Si noti che giochi basati sull'AI o filtri antispam non comportano rischi rilevanti e non rientrano nell'ambito di applicazione del regolamento.

[131] *Ibid.*

[132] M. Ozkan-Okay-E. Akin-Ö Aslan-S. Kosunalp-T. Iliev-I. Stoyanov-I. Beloev, *A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions*, in *IEEE Access*, 12, 2024, 12229 ss.

[133] M. Pawlicki-A. Pawlicka-R. Kozik-M. Choraś, *Advanced insights through systematic analy-*

strategico emergente nell'ambito giuridico-istituzionale. Dai *report* tecnici[134] e dalla normativa di settore è possibile ricavare tre principali direttrici dall'interazione tra le discipline dell'AI e della *cybersecurity*: (*i*) l'AI per la *cybersecurity*: l'AI applicata alla *cybersecurity* agisce come leva strategica per sviluppare sistemi integrati di gestione del rischio, misure di sicurezza avanzate e strumenti ad alte prestazioni di difesa e risposta alle minacce, risultando particolarmente efficace nel contrasto di fenomeni patologici quali, ad esempio, il *cybercrime* e l'*information disorder*; (*ii*) la *cybersecurity* dell'AI: la *cybersecurity* è una *precondizione essenziale* per garantire un uso corretto, trasparente e responsabile dell'AI grazie alla sua capacità di garantire una maggiore robustezza dei sistemi e dei modelli di AI e di mitigarne le vulnerabilità; (*iii*) l'uso malevolo dell'AI, dunque utilizzata con l'intento di nuocere a persone e *asset* strategici. L'AI in termini tecnici è spesso descritta come "moltiplicatore di forze" in quanto è capace di ampliare la superfice d'attacco e amplificare l'attacco informatico, generando minacce avanzate e non convenzionali [135] [136]. L'utilizzo malevolo dell'AI è di particolare interesse per le normative che si occupano di *cybercrime, cyber threat intelligence, cyber defence*, anche nella prospettiva del diritto internazionale. Queste direttrici, pur non essendo concetti giuridici tipizzati, sono riscontrabili nei più recenti strumenti normativi europei e nazionali. Infatti, in un'ottica di protezione multilivello delle infrastrutture critiche e della gestione del rischio *cyber* nelle organizzazioni, della sicurezza dei prodotti digitali e della *supply chain*, nonché della tutela dei diritti degli utenti e delle altre persone, le intersezioni normative tra le due discipline assumono sempre più rilievo. Se da un lato sia l'AI Act sia la Legge AI[137] assegnano una dimensione chiave alla sicurezza informatica, confermando il ruolo trasversale della materia e il rapporto virtuoso e multidimensionale esistente tra le due,[138] dall'altro non mancano riferimenti all'uso dell'AI nel

sis: Mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity, in *Neurocomputing*, 590, 2024, 127759.

[134] ENISA, *Report on Cybersecurity of AI and Standardization*, in *enisa.europa.eu*, marzo 2023; ENISA, *Securing Machine Learning Algorithms*, in *enisa.europa.eu*, dicembre 2021. NIST, *NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems*, in *nist.gov*, 4 gennaio 2024.

[135] G.F. Italiano-A. Martino-G. Piccardo, *Security and privacy in large language and foundation models: A survey on genai attacks*, in *International Conference on Distributed Computing and Intelligent Technology*, Cham, 2024, 1 ss.

[136] C. Nobles, *The weaponization of artificial intelligence in cybersecurity: A systematic review*, in *Procedia Computer Science*, 239, 2024, 547 ss.

[137] Per una panoramica della Legge AI nazionale, anche in connessione con altre normative digitali, si rimanda a G. Cassano-E. Prosperetti (a cura di), *Le regole dei dati e dell'intelligenza artificiale. Dal GDPR alla Legge 132/2025*, Santarcangelo di Romagna, 2025.

[138] ENISA, *Report on Cybersecurity of AI and Standardisation*, cit.

panorama normativo *cyber*.

3.1 L'intelligenza artificiale per la *cybersecurity*

La disciplina in materia di *cybersecurity* si caratterizza per un approccio di neutralità tecnologica, evitando di imporre l'adozione di tecnologie predeterminate e prescrivendo, piuttosto, che le misure di sicurezza implementate risultino proporzionate e adeguate ai rischi individuati. Nondimeno, le *policy* e le fonti normative di settore descrivono chiaramente il valore strategico delle *cybersecurity-enhancing technologies*, tra le quali l'AI, il cui impiego viene prospettato come elemento funzionale al rafforzamento complessivo della sicurezza dei sistemi informativi e di rete. In un'ottica di gestione del rischio integrata, i modelli di AI addestrati tramite tecniche di *machine learning*, [139] [140] [141] possono risultare particolarmente utili nella valutazione e nella classificazione del rischio all'interno delle reti per determinare la gravità di una vulnerabilità. Grazie alla capacità di analizzare grandi quantità di dati e di apprendere *pattern* complessi, queste tecnologie consentono di attribuire punteggi di rischio dinamici e contestualizzati, supportando le organizzazioni nel prioritizzare le azioni di mitigazione e migliorando la gestione complessiva del rischio *cyber*. A questo si aggiunga che, i modelli addestrati tramite tecniche di *machine learning*, consentono di identificare minacce e vulnerabilità con livelli di accuratezza e tempestività superiori rispetto agli approcci tradizionali.[142] Infine, i sistemi di AI migliorano le capacità delle organizzazioni nella predizione identificando *trend*, nonché nella risposta agli incidenti.[143]

La Strategia nazionale di *cybersicurezza* 2022-2026[144] considera lo sviluppo delle tecnologie di AI e di *machine learning* uno dei principali fattori abilitanti della crescita economica e della proiezione strategica del Paese. L'ACN, pur ricomprendendo tali tecnologie nell'ambito delle *Emerging and Disrup-*

[139] *Machine learning* (apprendimento automatico): disciplina scientifica, nell'ambito dell'intelligenza artificiale, che si pone l'obiettivo di sintetizzare modelli in grado di apprendere automaticamente da un insieme finito di dati tramite dedicati algoritmi di apprendimento.

[140] T. Mitchell, *Machine Learning*, New York, 1997.

[141] A.L. Samuel, *Some studies in machine learning using the game of checkers*, in *IBM Journal of research and development*, 3(3), 1959, 210 ss.

[142] ENISA, *Artificial intelligence and cybersecurity. ENISA Research and Innovation Brief*, in *enisa.europa.eu*, giugno 2023.

[143] A. Salvi-P. Spagnoletti-N.S Noori, *Cyber-resilience of Critical Cyber Infrastructures: integrating digital twins in the electric power ecosystem*, in *Computers & Security*, 112, 2022, 102507 ss.

[144] ACN, *Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026*, in *acn.gov.it*.

tive Technologies, evidenzia, al contempo, la necessità dualistica - difensiva e abilitante - di un impiego sinergico con la *cybersecurity*, come l'integrazione di questa tecnologia avanzata nei sistemi nazionali di monitoraggio e di analisi del rischio *cyber*, a supporto della sicurezza delle infrastrutture critiche nazionali.

Il Manuale operativo della Strategia di ACN[145] fornisce esempi concreti dell'applicazione di tali princìpi operativi: la gestione del rischio *cyber*, concepita in chiave preventiva e integrata su molteplici fonti di dati - comprese espressamente le tecnologie di AI e *machine learning* -, può supportare la *cybersecurity* nella funzione di «correlare e analizzare eventi di sicurezza di interesse».[146] L'impiego di strumenti integrati consentirebbe di creare una "super infrastruttura" ad alte prestazioni, con capacità elaborative sufficienti a «simulare, prevenire, scoprire, rispondere e predire gli impatti di attacchi *cyber* di natura sistemica».[147]

La normativa di derivazione unionale, come la Direttiva NIS2, invita i soggetti essenziali ed importanti a valutare l'impiego di tecnologie evolute, come l'AI e il *machine learning*, per il miglioramento delle proprie capacità e la sicurezza delle reti e dei sistemi informativi,[148] nel rispetto della protezione dei dati personali, dei principi di equità e trasparenza, e in combinazione con misure tecniche consolidate, quali la crittografia. Promuove, altresì, la ricerca e lo sviluppo in materia, sollecitando gli Stati membri a impiegare l'AI per potenziare le capacità di rilevamento delle minacce e prevenzione degli attacchi informatici[149]. Ciò può avvenire, ad esempio, tramite sistemi automatizzati o semiautomatizzati di rilevamento e di analisi predittiva delle minacce,[150] capaci di accrescere la rapidità della risposta e, conseguentemente, a mitigare gli effetti lesivi, siano essi di natura informatica o derivanti da altre forme di danno.

La normativa NIS2 lascia margine per un uso "mirato" dell'AI anche nello svolgimento delle competenze del CSIRT[151]. I CSIRT hanno, infatti, diverse possibilità per supportare le organizzazioni pubbliche e private,[152] e il gruppo italiano non fa eccezione, in quanto ha la facoltà di effettuare scan-

---

145 ACN, *Manuale operativo di attuazione della Misura 82. Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026*, su *acn.gov.it*.

146 Misura #30 in ACN, *Manuale operativo di attuazione della Misura 82*, cit.

147 Misura #32 in ACN, *Manuale operativo di attuazione della Misura 82*, cit.

148 Considerando 89, Direttiva NIS2.

149 Considerando 51, Direttiva NIS2.

150 G. Granato-A. Martino-A. Baiocchi-A. Rizzi, *Graph-based multi-label classification for WiFi network traffic analysis*. in *Applied Sciences*, 12(21), 2022, 11303 ss.

151 Art. 11, par. 3, lett. e), Direttiva NIS2.

152 I. Kamara-J. van den Boom, *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: Good practices*, 2022.

sioni proattive delle reti e dei sistemi informativi, su richiesta dei soggetti NIS italiani, per individuare vulnerabilità potenzialmente significative.[153] Si tratta di un'attività che potrebbe anche avvalersi di tecniche di AI e *machine learning*, sebbene la normativa non lo prescriva espressamente.[154]
L'Agenzia europea per la *cybersecurity* (ENISA) sintetizza le potenzialità dei sistemi basati sull'AI lungo tre direttrici: (*i*) la *detection*, ovvero l'identificazione di minacce e vulnerabilità; (*ii*) la *mitigation*, ossia la mitigazione delle minacce; (*iii*) la *prediction*, con riferimento alla capacità di anticipare rischi *cyber*[155].

3.2 La *cybersecurity* per l'intelligenza artificiale

La *cybersecurity* dell'AI è la direttrice con maggiori sviluppi paralleli sul piano tecnico e normativo. *Stricto sensu*, dal punto di vista tecnico, essa può essere intesa come l'insieme delle misure volte a garantire la protezione - in termini di riservatezza, integrità e disponibilità (c.d. triade CIA) - dei dati, dei modelli e dei processi che costituiscono un sistema di intelligenza artificiale lungo l'intero ciclo di vita. Tuttavia, il supporto della *cybersecurity* all'AI, non si esaurisce nella protezione dei sistemi AI da minacce ed attacchi, ma è la condizione preliminare per modelli e algoritmi di AI affidabili e sicuri, in quanto ne garantisce la robustezza, ne previene gli abusi e ne tutela l'affidabilità (*trustworthiness)*.
Affidabilità e robustezza sono due concetti interconnessi e la *cybersecurity* può garantirli entrambi. Un sistema di AI può dirsi robusto quando le sue prestazioni rimangono inalterate, nonostante una perturbazione da parte di un attaccante sui dati o su un modello di AI. Allo stesso tempo, un sistema di AI è affidabile quando, nel tempo, le sue prestazioni attese, corrispondono a quelle effettive.[156] Se attacchi *cyber* - come il *data poisoning*[157] e il *model poisoning*[158] - sono in grado di alterare le prestazioni del sistema, portandolo a comportamenti differenti da quelli attesi, la *cybersecurity* è in

[153] Art.15, par 3, lett. e), Decreto NIS2.

[154] I. Kamara-M. Bassini, *The cybersecurity and AI nexus in the EU digital acquis*, cit., 312 ss.

[155] ENISA, *Artificial intelligence and cybersecurity*, cit.

[156] L. Pupillo-S. Fantin-A. Ferreira-C. Polito, *Artificial intelligence and cybersecurity. Technology, Governance and Policy Challenges*, CEPS Task Force Report, maggio 2021.

[157] Protezione dei dati di addestramento da attaccanti malintenzionati che, qualora riuscissero a compromettere il *dataset*, potrebbero utilizzarlo come vettore di attacco verso il modello.

[158] Protezione del modello, una volta addestrato. I modelli sono composti da parametri che, se non opportunamente protetti, possono essere manipolati e compromessi da un attaccante con l'obiettivo di minare la sua affidabilità ed il suo potere predittivo. Si veda G.F. Italiano-A. Martino-G. Piccardo, *Security and privacy in large language and foundation models: A survey on genai attacks*, in *International Conference on Distributed Computing and Intelligent Technology*, cit.

grado di agire da scudo, ad esempio grazie all'utilizzo di misure di sicurezza quali la crittografia, capaci di rendere i dati intellegibili da chiunque (ad es. da chiunque agisca tramite un sistema informativo) e impenetrabili a tentativi di intrusione da parte di terzi non autorizzati. L'AI Act coglie questa capacità della sicurezza informatica - il testo conta oltre cinquanta riferimenti diretti – prevendendo un «obbligo di *cybersecurity*» come requisito necessario per i sistemi di AI ad alto rischio soggetti all'AI Act.[159] In particolare, l'art. 15 AI Act stabilisce che i sistemi di AI ad alto rischio debbano essere «progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e *cybersecurity* e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita». La medesima disposizione impone, inoltre, che tali sistemi siano resilienti a tentativi di terzi non autorizzati di alterarne l'uso o le prestazioni, attraverso misure quali ridondanza, piani di *fail-safe* e mitigazione dei rischi derivanti dai *feedback loops*. L'obbligo ad essere *cybersafe*, tuttavia, è circoscritto ai soli sistemi ad alto rischio.[160] D'altra parte, l'art. 12 CRA regolamenta i prodotti digitali che potrebbero incorporare sistemi di IA ad alto rischio, prevedendo una presunzione di conformità qualora ricorrano determinate condizioni.[161]
La *cybersecurity* è un principio cardine anche della Legge AI nazionale che la considera come una «precondizione essenziale» per garantire un uso corretto, trasparente e responsabile. I soggetti obbligati devono garantirla lungo l'intero ciclo di vita dei sistemi e modelli di AI per finalità generali, secondo un approccio proporzionato e basato sul rischio e l'adozione di adeguati controlli di sicurezza volti a garantire la resilienza dei sistemi e modelli di AI contro tentativi di manipolazione, alterazione delle prestazioni o modifiche delle impostazioni di sicurezza (art. 3, c. 6). La legge interviene, inoltre, sul piano istituzionale, ed in particolare sul d.l. 82/ 2021, convertito, con modificazioni, dalla l. 109/2021, ampliando le competenze di ACN, alla quale è affidato il compito di «promuovere e sviluppare ogni

[159] Cfr. art. 6 AI Act.

[160] Suscitando interrogativi circa l'assenza dell'obbligo di cybersecurity per gli altri sistemi di AI immessi sul mercato, come affermato da F. Bavetta-O. Pollicino, *Cybersecurity Requisiti tecnici e organizzativi solo per i sistemi ad alto rischio*, in *Il Sole 24 Ore*, 30 ottobre 2025.

[161] Il coordinamento tra CRA e AI Act emerge chiaramente dall'art. 12 CRA, che disciplina espressamente il rapporto tra prodotti con elementi digitali e sistemi di IA ad alto rischio. In particolare, la disposizione introduce una presunzione di conformità ai requisiti di *cybersecurity* di cui all'art. 15 AI Act per i prodotti che - rientrando nell'ambito di applicazione del CRA e qualificandosi come sistemi di IA ad alto rischio ai sensi dell'art. 6 AI Act - soddisfino i requisiti essenziali di *cybersecurity* previsti dal CRA. Tale presunzione opera al ricorrere di tre condizioni cumulative: (*i*) il rispetto dei requisiti essenziali di *cybersecurity* di cui all'allegato I, parte I, CRA; (*ii*) la conformità dei processi predisposti dal fabbricante ai requisiti di cui all'allegato I, parte II; (*iii*) la dimostrazione del livello di protezione richiesto dall'art. 15 AI Act mediante la dichiarazione di conformità rilasciata ai sensi del CRA.

iniziativa [...] volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della *cybersicurezza* nazionale» (art. 18). In questa dimensione, la *cybersecurity* svolge una funzione di supporto all'AI assumendo da un lato il suo tradizionale ruolo di *standard* tecnico, dall'altro evolvendosi per rispondere a sfide avanzate e contemporanee.
Le Linee guida per uno sviluppo sicuro dell'AI (2023),[162] promosse dal National Cyber Security Centre del Regno Unito, e sottoscritte da 23 Agenzie di diciotto Paesi, compresa l'ACN, evidenziano come i sistemi di AI - intese da questo strumento come le sole applicazioni di *machine learning* - siano soggetti a vulnerabilità nuove e peculiari, che si aggiungono a quelle tradizionali del dominio *cyber*, ad esempio l'*Adversarial Machine Learning* (AML): l'insieme delle tecniche che sfruttano le debolezze intrinseche dei modelli di apprendimento automatico - che possono riguardare sia componenti *hardware* e *software*, sia i flussi di lavoro e le catene di approvvigionamento - con l'obiettivo di indurre nei sistemi comportamenti non intenzionali o dannosi. I sistemi di AI sono, in fondo, sistemi informatici per questo ereditano tutti i rischi della sicurezza informatica connessi alle reti e ai sistemi informativi. Come la *cybersecurity*, anche l'AI sta evolvendo nel tempo ad una velocità molto rapida, tanto che l'attuale ecosistema AI è composto da una varietà di modelli e tecniche, con differenti livelli di maturità tecnologica: non tutti i modelli immessi sul mercato sono allo stesso stadio di sviluppo e non vengono utilizzati per gli stessi scopi.

4. Conclusioni

Le normative in materia di *cybersecurity* e intelligenza artificiale traducono il *risk management* in obblighi giuridici, orientando l'azione di soggetti pubblici e privati verso logiche proattive, proporzionate e anticipatorie del rischio.[163] Tuttavia, questo approccio si declina diversamente. La normativa *cyber* si fonda su un modello di gestione del rischio,[164] che valorizza la capacità del soggetto obbligato a valutarlo e gestirlo, nonché a identificare le vulnerabilità. L'AI Act opera, invece, una qualificazione normativa del rischio mediante una classificazione *ex ante* delle applicazioni di intelligenza artificiale in base al loro impatto sulla società, mantenendo una prospettiva esplicitamente antropocentrica a tutela dei diritti fondamentali e dell'autonomia umana.

---

[162] Si veda *Guidelines for secure AI system development*, in *acn.gov.it*.

[163] M.A. Rizzi-F. Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, cit.

[164] Sia questo basato sull' approccio tecnico-organizzativo e flessibile (NIS2, DORA) oppure integrato *by security e by design* nei prodotti digitali (CRA e, con le dovute specificità, anche il PSNC, ad esempio in relazione ai meccanismi di *procurement*).

In entrambe le discipline, *cyber* e AI, la sicurezza non può assurgere all'assenza assoluta di rischio,[165] bensì alla sua gestione informata, continua e proporzionata.[166] Il fine ultimo è prevenire eventi avversi, proteggere persone, diritti, interessi giuridici, organizzazioni e *asset*.[167] [168]
In questa prospettiva, ci si può interrogare, se dall'interpretazione della *cybersecurity law* - alla luce dell'interezza della normativa, tanto di derivazione unionale quanto domestica - non si possa desumere una lettura ulteriore superando il mero lessico tecnico adottato in sede di formazione dell'atto, [169] [170] e ricondur-

[165] Sarebbe, d'altronde, un obiettivo irrealistico in un ecosistema digitale intrinsecamente esposto a diverse complessità.

[166] Permettendo al diritto di distinguere tra rischio tecnico (es. un guasto o malfunzionamento), oggettivamente misurabile, e il rischio percepito che è legato a valutazioni soggettive e sensibili al contesto. V. F. Nocifora, *Sociologia della sicurezza, rischio e legalità democratica*, in AA.VV. (a cura di), *Sicurezza e democrazia*, Napoli, 2010, 101 ss.

[167] P. Cichonski-T. Millar-T. Grance-K. Scarfone, *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*, agosto 2012.

[168] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[169] Nell'analisi degli atti dell'Unione europea e della normativa derivata, occorre tener conto delle caratteristiche del processo legislativo e, in particolare, delle dinamiche negoziali che si sviluppano in seno al Consiglio dell'UE, nonché della composizione dei gruppi di lavoro, che incide sul risultato normativo. La rilevante prevalenza di esperti tecnici provenienti dai diversi Stati membri - quali ingegneri e specialisti della sicurezza informatica nel caso della *cybersecurity* - contribuisce alla produzione di testi nei quali il lessico operativo e il significato tecnico assumono un ruolo prevalente rispetto a quello propriamente giuridico. Ciò risulta ancor più evidente nelle fonti normative *cyber*, che tendono a mantenere una forte impronta tecnico-applicativa, sia sul piano concettuale sia su quello linguistico. Se, da un lato, tale impostazione favorisce un elevato grado di precisione operativa - come nel caso della nozione di "vulnerabilità" offerta dal CRA, dalla NIS2 e dal DORA - dall'altro richiede un'attività interpretativa volta a ricondurre tali concetti all'interno di un quadro giuridico più ampio, capace di coglierne le implicazioni nell'interezza del *framework*, e ricondurli a categorie giuridiche idonee a carpirne la rilevanza nel contesto della tutela dei diritti, della responsabilità e della regolazione del rischio nella società digitale. A titolo meramente esemplificativo e non esaustivo, si considerino il gruppo di lavoro orizzontale "Questioni riguardanti il ciberspazio" (*Horizontal Working Party on Cyber Issues – HWPCI),* istituito nel 2016, che coordina i lavori del Consiglio dell'Unione europea in materia di politiche e legislazione sulla *cybersecurity* e si riunisce con elevata frequenza - indicativamente più volte al mese -, e il gruppo orizzontale "Rafforzare la resilienza e contrastare le minacce ibride" (*Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats HWP ERCHT*) che si occupa di contrastare le minacce ibride, rafforzare la resilienza degli Stati e delle società a tali minacce e migliorare la comunicazione strategica e combattere la disinformazione. In tale contesto, ACN assicura un supporto soprattutto tecnico e strategico al Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI) e, in particolare, alla Rappresentanza Permanente d'Italia presso l'Unione europea (RappUE), contribuendo alla formazione della posizione italiana nei negoziati parte della procedura normativa, nonché contribuisce anche mediante «l'analisi di strumenti e opzioni operative». Si veda ACN, *Gruppo di Lavoro orizzontale sulle questioni cyber (HWPCI)* e *Hybrid e altri gruppi di lavoro UE*, in *acn.gov.it*.

[170] A tali criticità si aggiungono ulteriori fattori che contribuiscono ad accrescere la com-

la a categorie giuridiche idonee a coglierne la rilevanza nel contesto della tutela dei diritti, della responsabilità e della regolazione del rischio nella società digitale. Non si tratta di cristallizzare il lessico in costrutti rigidi, poco compatibili con la dinamicità e la complessità della materia, bensì di renderlo più adattivo e sensibile, tramite una lettura inferenziale, alle esigenze giuridiche, sociali e al contesto storico di riferimento, caratterizzato da una continua evoluzione tecnologica ed un'elevata produzione normativa sul digitale. In questo modo, sarebbe il diritto innanzitutto, e non la tecnica, a definire meglio gli spazi e i confini della materia stessa. A questa premessa segue la domanda se sia possibile ricavare una nozione di *cyber vulnerability*, che assume un significato peculiare per le normative considerate e che trascende la mera definizione normativo-nozionistica di "vulnerabilità" contenuta nella *cybersecurity law*[171].

La *cyber vulnerability* deve essere intesa come una condizione di potenziale esposizione che precede e struttura il rischio e ne consente la qualificazione. La consapevolezza delle vulnerabilità consente al soggetto obbligato, infatti, di individuare e prioritizzare gli *asset*, le funzioni e i diritti suscettibili di compromissione, permettendo una prima classificazione rilevante ai fini della loro tutela. In altre parole, assume una funzione ordinante in un ambito caratterizzato da multifattorialità ed elevata complessità tecnica.

In tal senso, la *cyber vulnerability* costituisce il presupposto logico-giuridico, non statico, dell'approccio *risk-based*, orientando le attività di *compliance* dei soggetti obbligati. Essa si manifesta come una condizione diffusa e sistemica, che attraversa l'intero ecosistema digitale, coinvolgendo le reti e i sistemi informativi. La compromissione dell'*availability* e dell'*integrity* delle infrastrutture critiche, così come delle condizioni di sicurezza dei prodotti digitali, può peraltro avere conseguenze sull'accesso a servizi essenziali.

Ne deriva che la *cybersecurity law* va oltre al mero obiettivo tecnico assumendo un ruolo funzionale, trasversale e complementare rispetto ad altri ambiti normativi – dalla protezione dei dati personali, alla regolazione dell'intelligenza artificiale – configurandosi, così, come uno *standard* da raggiungere per la tutela dei diritti dell'individuo nella società digitale.

Il tecnocentrismo della normativa *cyber* non è, dunque, fine a sé stesso: l'essere umano resta il soggetto esposto ai rischi derivanti dall'uso della tecnologia. Le minacce informatiche colpiscono primariamente componenti tecnologiche, ma incidono su aspetti fondamentali dell'esistenza dell'individuo (come

plessità, tra cui le traduzioni ufficiali degli atti normativi, che in alcuni casi divergono dal lessico adottato a livello domestico. Emblematico è il caso della pluralità terminologica utilizzata per indicare la cybersecurity - *cybersecurity*, *cibersecurity*, *sicurezza informatica*, *cybersicurezza*, *cibernetica*- che riflette non solo differenti scelte linguistiche, ma anche disallineamenti concettuali e interpretativi.

[171] Nozione di derivazione tecnica che rimanda alla debolezza di sistemi, prodotti o servizi ICT. Cfr. *supra*.

la sua vita privata, la sua attività lavorativa e imprenditoriale, l'accesso ai servizi pubblici digitali, la gestione della propria identità digitale, la sicurezza dei dati bancari e dei sistemi di pagamento, la continuità dei servizi essenziali, la partecipazione ai processi democratici, l'accesso all'istruzione, nonché la tutela della reputazione personale e professionale nell'ambiente informativo digitale). In tale prospettiva l'interesse protetto rimane eminentemente umano e sociale, poiché gli incidenti *cyber* possono tradursi in limitazioni concrete dell'autonomia individuale. La *cyber vulnerability*, in questo senso, non riguarda soltanto le debolezze tecniche e lo *human factor* (possibilità di commettere errori), ma comprende in modo sostanziale anche la vulnerabilità dell'essere umano, intesa come condizione soggettiva dell'esistenza, di esposizione al rischio. Nel discorso giuridico, invero, la vulnerabilità si configura come un concetto polisemico che dipende dal contesto. Più che indicare una condizione univoca e definita, essa assume una connotazione flessibile in quanto è utilizzata trasversalmente, in diversi ambiti del diritto, per evidenziare asimmetrie strutturali tra soggetti deboli e forti, richiamando una responsabilità giuridica di protezione.[172]

Nella *cybersecurity law*, tuttavia, la *cyber vulnerability* assume una dimensione peculiare, in quanto oltre che soggettiva è anche universale: tutti i soggetti risultano potenzialmente esposti innanzi al digitale e dunque vulnerabili. Il diritto, in questo caso, non è chiamato a proteggere solo determinate categorie specifiche di soggetti (es. i minori, i disabili)[173], ma a garantire condizioni di sicurezza per l'intera società.[174] In questa prospettiva, la tutela delle persone e della società dal rischio tecnologico – incluso quello *cyber* – costituisce l'orizzonte verso cui i sistemi di *risk governance*, delineati dalla normativa, devono convergere.

---

[172] F. Panuccio Dattola-T. Amodeo, *Vulnerabilità e diritti umani: strumenti e percorsi di tutela*, Milano, 2022.

[173] Cfr. l'art. 5 AI Act, il quale prevede il divieto di «immissione sul mercato, la messa in servizio o l'uso di un sistema di AI che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone», in quanto queste tecniche di manipolazione possono essere utilizzate per persuadere l'utilizzatore ad adottare comportamenti indesiderati o per indurre le persone a prendere decisioni con l'inganno, sovvertendone e pregiudicandone l'autonomia, il processo decisionale e la libera scelta. Il rischio individuato dalla normativa è quello di «causare danni significativi sulla salute fisica, psicologica o sugli interessi finanziari», ancor più se si tratta di persone ritenute particolarmente fragili, che il regolamento definisce indirettamente, come persone o gruppi di persone che «versano in condizione di vulnerabilità dovute all'età, a disabilità… o a una specifica situazione sociale o economica che potrebbe renderle più vulnerabili allo sfruttamento, come le persone che vivono in condizioni di povertà estrema e le minoranze etniche o religiose» (considerando 29).

[174] La consapevolezza di questa vulnerabilità universale «deve fondare l'attività legislativa e le istituzioni sociali, e cioè l'impegno della legalità, dell'organizzazione della società e delle sue leggi nel proteggere la società». T. Amodeo, *Tutela e protezione di soggetti vulnerabili. Un nuovo progetto di vita: il co-housing*, in *Judicium.it*, febbraio 2021.

Abstract

Il presente contributo ricostruisce e analizza la *governance* della *cybersecurity* nel quadro normativo europeo e nazionale, mettendo in luce le complementarità tra modelli integrati orientati alla sicurezza delle reti, dei sistemi e dei prodotti ICT. In tale contesto, si esamina la relazione virtuosa tra *cybersecurity* e intelligenza artificiale, sia nella prospettiva dell'AI per la *cybersecurity* quale strumento di prevenzione, rilevazione e risposta alle minacce, efficace soprattutto nel contrasto di fenomeni patologici, sia della *cybersecurity* per l'AI quale precondizione necessaria per garantire affidabilità, sicurezza e robustezza dei sistemi, mitigandone le vulnerabilità. Il contributo, infine, introduce il concetto di *cyber vulnerability* quale condizione di esposizione che precede e struttura il rischio. In tale prospettiva, la *cybersecurity law* emerge come strumento trasversale di tutela nella società digitale.

This paper examines and analyzes cybersecurity governance within the European and national regulatory frameworks, highlighting the complementary nature of integrated models focused on the security of networks, systems, and ICT products. In this context, it examines the virtuous relationship between cybersecurity and artificial intelligence, both from the perspective of AI for cybersecurity as a tool for prevention, detection, and response to threats - effective above all in combating malicious phenomena – as well as from the perspective of cybersecurity for AI as a necessary precondition for ensuring the reliability, security, and robustness of systems, thereby mitigating their vulnerabilities. Finally, this paper introduces the concept of cyber vulnerability as a condition of exposure that precedes and shapes risk. From this perspective, cybersecurity law emerges as a cross-cutting tool for protection in the digital society.

Keywords

cyber vulnerability - cybersecurity law - artificial intelligence regulation - risk-based approach - standard