Cybersicurezza e Intelligenza Artificiale. Un'analisi critica

Raffaella Brighi*

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE. A CRITICAL ANALYSIS

ABSTRACT: The increasing complexity of cyber threats calls for the continuous evolution of cybersecurity strategies. This contribution explores the role of artificial intelligence (AI) in cyber- protection and defence, in particular, taking into account the revolution of cybersecurity practices brought about by advanced techniques such as machine learning and deep learning. The analysis of European and Italian strategies highlights the importance of an integrated approach involving technology, regulation and stakeholder cooperation. The risks related to the use of AI, including new vulnerabilities and potential ethical and social implications, are also discussed, with a view to analysing solutions for a more secure and resilient digital future.

KEYWORDS: Cybersecurity; Resilience; Artificial intelligence; Risk; EU Law.

ABSTRACT: La crescente complessità delle minacce informatiche impone un'evoluzione continua delle strategie di cybersicurezza. Il contributo esplora il ruolo dell'Intelligenza Artificiale (IA) nella protezione e nella difesa cibernetica, evidenziando come tecniche avanzate quali il *machine learning* e il *deep learning* stiano rivoluzionando il campo. Analizzando le strategie europee e italiane, si evidenzia l'importanza di un approccio integrato che coinvolga tecnologia, normativa e cooperazione tra gli stakeholder. Vengono inoltre discussi i rischi legati all'uso dell'IA, incluse le nuove vulnerabilità e le potenziali implicazioni etiche e sociali, analizzando soluzioni per un futuro digitale più sicuro e resiliente.

PAROLE CHIAVE: Cybersicurezza; Resilienza; Intelligenza Artificiale; Rischio; EU Law.

* *Professoressa Associata di informatica giuridica, Università di Bologna. Mail. Raffaella.Brighi@unibo.it.* *La ricerca è stata svolta nell'ambito del progetto PNRR "Partenariato Esteso" SERICS (PE00000014) – EcoCyber, Spoke 8, Finanziato dall'Unione europea – Next Generation EU ed anche nell'ambito del progetto ERC Computable Law ("CompuLaw") - Grant Agreement 833647. Contributo sottoposto a doppio referaggio anonimo.*

ISSN 2284-4503

1. Insicurezza informatica. Minacce, vulnerabilità e nuovi rischi

La cybersicurezza rappresenta una sfida di primaria importanza nella nostra società digitale. Il costante aumento delle minacce e degli incidenti informatici, insieme alla sempre maggiore area di esposizione, ha spinto governi e istituzioni a promuovere strategie di resilienza e misure di protezione avanzate che comprendono, oltre alla tecnologia, interventi normativi, politici, economici e sociali[1].

L'Unione Europea ha riconosciuto l'importanza della cybersicurezza vedendola come elemento abilitante alla trasformazione digitale. Questo si è tradotto nell'emanazione di tre diverse *Strategie* che, sin dal 2013, promuovono un approccio di tipo globale, basato sulla cooperazione internazionale, la condivisione di informazioni e la redistribuzione di responsabilità tra settore pubblico e privato[2]. In questo quadro, sono stati adottati o proposti diversi atti giuridici che lungo tre macroaree di intervento – la resilienza, il contrasto al cybercrimine, la cyberdifesa e la cyberdiplomazia – definiscono un nuovo assetto normativo in materia di *cybersecurity*[3]. In Italia, la creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) nel 2021, all'interno del Piano Nazionale di Ripresa e Resilienza (PNRR), rappresenta un passo significativo verso un sistema di sicurezza più coordinato e robusto[4].

Le minacce informatiche colpiscono un'ampia gamma di soggetti, dai privati cittadini alle grandi aziende, fino agli enti pubblici e le istituzioni governative considerato che ogni aspetto della vita quotidiana – dai servizi pubblici all'istruzione, dal lavoro all'economia e ai processi democratici – dipende da reti, sistemi e tecnologie informatiche in costante evoluzione. Se da un lato l'irreversibile digitalizzazione di attività e servizi rende evidente l'importanza cruciale della sicurezza informatica come ele-

[1] *Ex multis*, T.F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni Costituzionali*, 2, 2024; R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano, 2023; E.C. Raffiotta, *Cybersecurity Regulation in the European Union and the Issues of Constitutional Law*, in *Rivista AIC*, 4, 2022; F. Casarosa, G. Comandé, *Aspettando la NIS2: ovvero il diritto privato della Cybersecurity*, in *Il Diritto dell'informazione e dell'Informatica*, XL, 1, 2024; S. Pietropaoli, *Cybersecurity in Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, 2023, 99-114.

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

[3] Un primo ambito del nuovo assetto riguarda il rafforzamento della sicurezza delle reti e dei sistemi informativi per incrementare la *cyber resilienza* nei settori essenziali per l'economia e la società, sia pubblici che privati, con l'emanazione della Direttiva NIS (*Network and Information Security* – Direttiva (UE) 2016/1148) e la sua revisione, la Direttiva NIS2 (Direttiva (UE) 2022/2555), la Direttiva CER (*Critical entities resilience directive*, Direttiva (UE) 2022/2557) e il regolamento DORA (*Digital operational resilience act* - Regolamento (UE) 2022/2554). Un secondo ambito riguarda la creazione di un quadro europeo di certificazione della cybersicurezza, tramite il Cybersecurity Act (Regolamento (UE) 2019/881), volto a garantire alti standard di sicurezza per prodotti, servizi e processi ICT con un approccio di sicurezza by design. La promozione della sicurezza sin dalla fase di progettazione è ulteriormente concretizzata nella proposta di nuove norme orizzontali per i prodotti con elementi digitali, attraverso il Cyber Resilience Act, approvato nel marzo 2024. Infine, un terzo ambito prevede la creazione di un 'ciberscudo europeo', attraverso prima la specificazione e il potenziamento del ruolo dell'ENISA, poi con la proposta del c.d. Cyber Solidarity Act (18 aprile 2023), che attraverso quadri di cooperazione operativa già esistenti (EU-CyCLONe e la rete di CSIRTs), intende rafforzare la capacità della UE di prepararsi e gestire gli attacchi su larga scala.

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

mento fondamentale per la trasformazione economica e sociale, d'altro canto siamo ancora lontani dal raggiungere un livello di protezione adeguato[5].

In aggiunta a rischi noti quali disuguaglianze, discriminazioni, controllo sociale e concentrazione del potere digitale, le tensioni geopolitiche e i conflitti in corso hanno reso evidente che il rischio cibernetico è globale e di primaria importanza. Attacchi informatici sempre più sofisticati e aggressivi possono veicolare ulteriori gravi pericoli, come il terrorismo internazionale, conflitti tra Stati, attività economiche illecite, campagne di disinformazione. Tali minacce, in grado di colpire «sia gli interessi dello Stato che la fruibilità dei diritti dei soggetti di un ordinamento»[6], hanno ridefinito natura e confini dello stesso concetto di sicurezza pubblica[7]. In questo contesto, gli Stati sempre di più trattano il tema della cybersicurezza come una questione intrinsecamente connessa alla tutela della sicurezza nazionale.

In tal senso, è emblematico il caso dell'Italia che nel 2019 si dota di un autonomo quadro normativo in materia – nelle more del processo di revisione della direttiva UE 2016/1148 (cd. direttiva NIS) – al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di soggetti pubblici e privati, da cui dipende l'esercizio di una funzione o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento possa derivare un pregiudizio per la sicurezza nazionale[8]. Peraltro, il nostro legislatore, con il decreto di istituzione di ACN, nel definire il perimetro della cybersicurezza ha richiamato tra gli obiettivi anche la «tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico»[9]. In definitiva, si tratta di una funzione di sicurezza che interessa complessivamente l'ordinamento statale e le sue componenti, ossia le imprese e i singoli cittadini, dove la complessità della materia e la necessità di coordinamento tra le istituzioni coinvolte e le imprese che operano nel settore, richiamano un intervento ampio, multilivello e trasversale[10].

Il report dell'ENISA (*European Union Agency for Cybersecurity*) – *Foresight Cybersecurity Threats for 2030* – nell'identificare le dieci principali minacce che peseranno sul cyberspazio nel 2030[11], sottolinea l'importanza della implementazione di politiche di mitigazione dei rischi per aumentare la sicu-

[5] Il Rapporto Clusit 2024 sulla sicurezza ICT in Italia evidenzia che il 64% degli incidenti hanno come causa azioni "maldestre", degli utenti o del personale ICT. Malware, Vulnerabilità, Phishing e Account Cracking sono indice di carenze nella cyber igiene degli utenti che restano vulnerabili alle tecniche di più comuni di ingegneria sociale.

[6] G. De Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, In *Rivista AIC*, 4, 76.

[7] Sul punto si vedano T.F. Giupponi, *Sicurezza e potere*, in *Enciclopedia del diritto*, *I tematici*, V, 1146 ss.; G. De Vergottini, *op cit.*, 65 ss.

[8] Decreto-legge n. 105 del 2019, convertito con modificazioni dalla legge 4 novembre 2019, n. 133.

[9] F. Serini, *La nuova architettura della cybersicurezza nazionale: note a una prima lettura del decreto-legge n.82 del 2021*, in *Federalismi.it*, 12, 241 ss.

[10] In argomento, si vedano T.F. Giupponi, *Il governo nazionale della cybersicurezza,* cit., 180-181; R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in R. Ursi (a cura di), cit., 13 ss.

[11] Tra queste la compromissione della supply chain a causa della vulnerabilità dei molteplici componenti *hardware* e *software* integrati nei nuovi prodotti digitali, la manomissione dei dispositivi cyberfisici per lo sfruttamento di dati comportamentali e sensibili degli individui, l'abuso di sistemi di intelligenza artificiale attraverso la manipolazione intenzionale degli algoritmi e dei dati di addestramento.

rezza e la resilienza delle infrastrutture su cui si fonderanno le città del futuro. Esiste una asimmetria evidente tra il lato della difesa e quello dell'attacco. Il compito della difesa è notevolmente più complesso e richiede interventi su molteplici livelli. Mentre gli attaccanti possono sfruttare vulnerabilità specifiche e nuove tecniche, i difensori devono proteggere una vasta gamma di sistemi, applicazioni e dati, in modo proattivo, prevedendo potenziali minacce e adottando misure preventive.

Tra le principali innovazioni tecnologiche, l'intelligenza artificiale (IA) sta emergendo come una risorsa chiave nella lotta contro le minacce informatiche, rivoluzionando anche il campo della cybersicurezza. Tecniche avanzate come il *machine learning* (ML) e il *deep learning* (DL) migliorano per rapidità ed efficacia la capacità di analisi dei dati di sicurezza e di decisione autonoma. Queste tecnologie potenzieranno la capacità difensiva con nuovi metodi per prevenire, rilevare e rispondere agli attacchi informatici.

Tuttavia, in ragione della natura *dual use* della IA, comune a molte tecnologie, la stessa è annoverata anche tra i pericoli emergenti per la sicurezza informatica. L'IA infatti amplifica le capacità di attacco, fornendo strumenti agli aggressori che arricchiscono il panorama di nuove minacce in termini sia quantitativi sia qualitativi. Inoltre, anche questi i sistemi non sono esenti da vulnerabilità intrinseche che possono portare ad errori o essere sfruttate in molti modi, tra cui attacchi in grado di avvelenare i dati di addestramento (*data poising*) o raggirare il *prompt* delle IA generative[12].

Questo incremento di complessità crea ulteriori vulnerabilità e potenzia le azioni malevole, rendendo la sicurezza informatica una sfida sempre più articolata.

Per sfruttare appieno l'applicazione dell'intelligenza artificiale nella cybersicurezza, gli attori, governativi o privati, devono padroneggiare gli strumenti e saperne comprendere e affrontare i rischi, per promuovere un utilizzo responsabile e sicuro. Le specificità di natura tecnica dell'AI, quali opacità e *bias* algoritmici, unite alla raccolta e analisi massiva di dati personali e comportamentali, pongono criticità rispetto all'automazione dei processi di difesa informatica che devono essere affrontati sul piano tecnico, normativo e sociale.

In tale contesto, questo contributo intende esplorare l'impatto dell'IA nel miglioramento della cybersicurezza, sia a livello individuale che collettivo. La prossima sezione introduce i paradigmi metodologici della sicurezza informatica, la sezione 3 analizza gli scenari in cui l'IA viene impiegata per automatizzare e rendere più efficaci i controlli di sicurezza, la sezione 4 si soffermerà sul *dual use* della tecnologia in esame e sulle nuove vulnerabilità per avanzare alcune riflessioni sul futuro della AI nella cybersicurezza.

2. Fondamenti tecnico-giuridici della cybersicurezza

L'espressione *cybersecurity* è definita dal Cybersecurity Act (Regolamento (UE) 2019/881) come l'«insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche». Ad un alto livello di astrazione essa si estrinseca nello studio, progettazione e implementazione di strategie volte a proteggere la dimensione digitale da un pericolo (o dalla minaccia di un pericolo) di natura volontaria o accidentale[13].

[12] Infra § 4.

Le attività riguardano limitatamente l'adozione di strumenti tecnologici quanto, piuttosto, la definizione di politiche (norme, regole amministrative e procedure organizzative), la predisposizione di meccanismi di controllo e la promozione di comportamenti individuali corretti. Tra queste strategie rientrano procedure di autenticazione, gestione degli accessi, analisi dei rischi, aggiornamento dei sistemi, rilevazione e reazione ad incidenti o attacchi, recupero delle componenti oggetti di attacco, addestramento e formazione del personale.

La progettazione efficace della sicurezza - attraverso procedure, controlli, comportamenti e tecnologie - è guidata dal *controllo del rischio* [14]. La regolazione e la gestione del rischio permea tutta la disciplina della sicurezza informatica e è alla base della più recente legislazione della UE in materia [15]. Non solo rischi per reti e sistemi informativi, ma anche rischi sociali, rischi per l'integrità fisica, rischi per i diritti e le libertà fondamentali: la normativa europea ha in sostanza ampliato il concetto di cybersecurity per includere la governance di un'ampia gamma di rischi, senza concettualizzarlo in modo impropriamente limitato. Il grado di esposizione al rischio, la probabilità che si verifichino incidenti e lo loro gravità sono i parametri in base ai quali determinare l'adozione di misure di sicurezza informatica conformi allo stato dell'arte e agli standard europei (ETSI, CEN) e internazionali (ISO/IEC), gli obblighi di segnalazione degli incidenti e l'adesione a quadri di certificazione della conformità. Le aree in cui si articolano le attività sono sostanzialmente tre: (i) realizzare sistemi robusti in grado di resistere agli attacchi, (ii) progettare metodi per il rilevamento di minacce ed anomalie al fine di garantire la resilienza dei sistemi; (iii) definire le risposte agli attacchi per ripristinare sistemi e servizi [16]. La robustezza dei sistemi è essenziale per mitigare l'impatto degli incidenti, consente alle infrastrutture e ai servizi nazionali critici di funzionare e ai cittadini di fare affidamento su tecnologie sicure. La resilienza e la risposta sono invece il lato attivo della sicurezza informatica che, a questo scopo, si avvale di forme di monitoraggio della rete per identificare attacchi e fonti di attacchi e reagire alle minacce. Ciascuna area comprende una vasta gamma di soluzioni tecniche e misure organizzative.

Alcuni *framework* di riferimento per il settore forniscono un insieme di linee guida standard e *best practice*, richiamate anche dal quadro normativo in materia, che aiutano le organizzazioni a uniformare le pratiche di sicurezza e facilitano comunicazione e cooperazione. Tra tutti, è rilevante per le nostre analisi il modello NIST[17] perché, oltre a essere molto noto nella comunità scientifica, è alla base del *Framework Nazionale per la Cybersecurity e la Protezione dei Dati*[18] e della tassonomia

[13] Per un'analisi del concetto di cybersecurity, V. PAPAKONSTANTINOU, *Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity*?, *44 Computer Law & Security Review*, 2022; M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds and Machines*, 29, 3, 2019, 349-354; R. BRIGHI, P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *Federalismi*, 2021, 21, 18-42; G. ZICCARDI, *La Cybersecurity nel quadro tecnologico (e politico) attuale*, in *Tecnologia e Diritto*, III, Milano, 2019, 207-210.

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

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

[16] G. D'ANGELO, G. GIACOMELLO, *Cybersicurezza. Che cos'è e come funziona*, Bologna, 2023.

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

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

adottata dal decreto attuativo del Perimetro Nazionale di Sicurezza Cibernetica (PSNC), dpcm 14 aprile 2021, n. 81 in materia di notifiche degli incidenti e misure di sicurezza.
Data l'eterogeneità delle soluzioni di cybersicurezza e la molteplicità delle applicazioni di IA che stanno emergendo, introdurre una tassonomia uniforme, accettata e consolidata è utile per tracciare una visione sistematica di opportunità e rischi dell'applicazione della IA alle strategie di cybersicurezza.
La tassonomia del NIST definisce cinque funzioni chiave per il processo di gestione della cybersicurezza nel tempo: identificazione, protezione, rilevamento, risposta e ripristino. La fase di *identificazione* si concentra sull'individuazione delle criticità e dei rischi associati a sistemi, dati, asset e persone, fornendo le basi per le successive fasi di gestione. La *protezione* si occupa di implementare controlli adeguati a prevenire o contenere l'impatto di eventi negativi e attiene alla robustezza del sistema. La *rilevazione* è dedicata all'identificazione tempestiva di incidenti di sicurezza attraverso il monitoraggio continuo e l'analisi delle anomalie. La *risposta* prevede le attività necessarie per intervenire quando un incidente viene rilevato, con l'obiettivo di contenerne l'impatto. Infine, il *ripristino* riguarda la gestione dei piani per recuperare rapidamente la funzionalità dei processi e dei servizi colpiti da un incidente, garantendo la resilienza delle infrastrutture. Per ogni funzione chiave si sono sviluppate e sono riprese metodologie consolidate, strumenti tecnologici, raccomandazioni e strategie organizzative che includono, qualora il contesto lo richieda, anche i vincoli legali.

3. Applicazioni dell'IA a supporto della cybersicurezza

L'aumento del numero, della portata e dell'impatto degli attacchi informatici necessita di una difesa dinamica, proattiva e adattativa, supportata da valutazioni in tempo reale attraverso il monitoraggio continuo e l'analisi dei dati.
La letteratura tecnico-scientifica è concorde nel rilevare che l'intelligenza artificiale viene sempre più integrata nel tessuto della cybersecurity e utilizzata in una varietà di scenari applicativi[19]. Per risolvere i problemi di cybersecurity di oggi sono impiegate diverse tecniche di IA, in particolare l'apprendimento automatico (supervisionato, per rinforzo e non-supervisionato), algoritmi di elaborazione del linguaggio naturale (NLP, *Natural Language Processing*), sistemi di rappresentazione della conoscenza, sistemi per la descrizione e modellazione del ragionamento, sistemi di ragionamento basati sui casi[20].
Esiste un'ampia gamma di tecniche di difesa che possono essere abilitate dall'IA con il potenziale di fornire prestazioni soddisfacenti a basso costo e in tempo reale per la sicurezza delle reti e dei dati, la protezione degli *endpoint*, l'affidabilità degli accessi, il rilevamento, l'identificazione e la mitigazione dei cyberattacchi. In particolare, alcuni studi esplorano le applicazioni della IA e le tendenze di ricerca

[19] In particolare si veda M. Malatji, A. Tolah, *Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI*, in *AI Ethics* (2024); I.H. Sarker, et al., *AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions*, in *SN Computer Science*, 2, 173 (2021); J. Edwards; W. Griffin, *Artificial Intelligence in Cybersecurity* in *The Cybersecurity Guide to Governance, Risk, and Compliance*, Wiley, 2024, 497-510; R. Kaur, D. Gabrijelčič, T. Klobučar, *Artificial intelligence for cybersecurity: Literature review and future research directions*, in *Information Fusion*, 97, 2023,101804.
[20] Per la classificazione dei sistemi di intelligenza artificiale cfr. S. Russel, P. Norvig, *Artificial Intelligence: A Modern Approach*, Prentice Hall Press, 2009; G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022.

mappandole secondo la tassonomia del NIST, introdotta nella sezione 2, e forniscono una panoramica sistematica dello stato dell'arte in questo campo[21]. Secondo i dati raccolti la maggior parte delle applicazioni di IA che integrano i metodi di sicurezza convenzionali riguardano la fase di rilevamento, un numero minore si occupa dell'identificazione, a seguire protezione e risposta. Poche sono le ricerche e gli strumenti focalizzati sull'applicazione della IA nelle operazioni di ripristino dei sistemi.

A supporto dei processi decisionali nella fase di rilevamento, l'intelligenza artificiale migliora la comprensione delle minacce informatiche tramite l'estrazione automatica, la correlazione e la valutazione di informazioni da molteplici fonti eterogenee, quali database di vulnerabilità, social media, siti di notizie, rapporti sugli incidenti e dark web. Nei sistemi di rilevamento delle intrusioni (IDS), tecniche di ML e DL permettono di analizzare il traffico di rete, rilevare attività sospette, classificare gli eventi e distinguere tra vari tipi di attacchi[22]. Analogamente, l'IA rivela anomalie su sistemi informativi e dispositivi fornendo una visione chiara e dinamica dell'ambiente cyberfisico[23] e, nell'ambiente, dei comportamenti degli utenti interni all'organizzazione.

Con riferimento alla fase di *identificazione*, strumenti di IA gestiscono gli *asset* nelle reti estese, scoprendo e configurando automaticamente dispositivi, applicazioni e utenti del sistema attraverso tecniche di clustering e ML. Sistemi di riconoscimento biometrico fisico e comportamentale sfruttano l'IA per il controllo dell'identità; i modelli di comportamento d'uso, relativi all'interazione dell'utente con il proprio dispositivo e le statistiche delle interazioni con diverse applicazioni, consentono ad esempio di determinare se l'utente corrente sia lo stesso di quello precedentemente autenticato (autenticazione continua).

L'IA previene la perdita dei dati identificando e classificando informazioni in base a caratteristiche condivise, monitora l'attività degli utenti interni per rilevare comportamenti anomali rispetto ai modelli elaborati sulla base del pregresso, aiuta a bloccare le mail di spam e di phishing e con esse i potenziali pericoli, può scoprire *malware* emergenti che generano varianti per eludere gli approcci tradizionali basati su regole e può individuare contenuti digitali alterati (*deep fake*)[24]. La formazione e la sensibilizzazione adattiva offrono contenuti aggiornati e personalizzati, migliorando la consapevolezza e le competenze degli utenti.

La funzione di *risposta* nella cybersecurity è essenziale per gestire e contenere l'impatto degli eventi di sicurezza. L'intelligenza artificiale introduce miglioramenti significativi automatizzando processi complessi e riducendo il carico di lavoro degli analisti[25] con strumenti di gestione dinamica dei casi

[21] R. Kaur, D. Gabrijelčič, T. Klobučar, *op.cit.*

[22] A. Venturi, G. Apruzzese, M. Andreolini, M. Colajanni, M. Marchetti, *DReLAB - Deep REinforcement Learning Adversarial Botnet: A benchmark dataset for adversarial attacks against botnet Intrusion Detection Systems*, in *Data in brief*, 34, 2021, 1-12.

[23] G. Gori, L. Rinieri, A. Melis, A. Al Sadi, F Callegati, M. Prandini, *A Systematic Analysis of Security Metrics for Industrial Cyber–Physical Systems*, in Electronics S, 13(7), 2024, 1-17.

[24] L. Guarnera, O. Giudice, S. Battiato, *Fenomenologia dei Deepfake: aspetti teorici e operativi per la detection di volti umani "artificiali"*, in R. Brighi (a cura di), *Nuove questioni di informatica forense*, Roma, 2022.

[25] M. Ferrazzano, *L'intelligenza artificiale a servizio delle attività di informatica forense*, in *Ordines*, 2, 2023, 132-146; S. Costantini, G. De Gasperi, R. Olivieri, *Digital forensics and investigations meet artificial intelligence*, in *Annals of Mathematics and Artificial Intelligence*, 86/2019, 193-229.

che registrano scenari di attacco e suggeriscono azioni di risposta appropriate basate sulle lezioni apprese dagli incidenti pregressi.

Nella fase di *ripristino*, l'intelligenza artificiale può automatizzare il recupero dei dati e dei sistemi e può supportare i processi di pianificazione della risposta futura con l'esame delle strategie esistenti e con l'analisi e aggregazione dei dati sugli incidenti e i registri di audit.

L'IA sta, dunque, diventando sempre più essenziale nello sviluppo di strumenti per perseguire gli obiettivi di sicurezza informatica e far fronte alle minacce emergenti. Le soluzioni tecnologiche qui descritte integrano la capacità di apprendimento automatico e profondo per elaborare, in modo più efficace e più veloce rispetto alle persone, grandi flussi di dati e ricavare informazioni che possono essere rilevanti in tutte le fasi della sicurezza informatica, dall'analisi del contesto per la progettazione delle misure di protezione fino al ripristino dei sistemi e servizi. La combinazione di Big Data e IA consente di automatizzare processi di decisione complessi, basati su numerosi fattori e criteri non esattamente predeterminati. Ciò può migliorare la qualità delle decisioni pubbliche e private, ma impone di riflettere sui rischi, collegati alle specificità tecniche dei sistemi di IA (tra cui *bias* algoritmici, opacità, scelta del *dataset*), che sono oggetto del dibattito dottrinale più recente[26].

Raccolta, conservazione e analisi massiva dei dati di sicurezza sono essenziali per lo sviluppo di strumenti di difesa cibernetica basati su IA. Dalla *threat intelligence* per scopi predittivi all'automazione totale dei processi di risposta, questi sistemi utilizzano grandi quantità di dati, tra cui dati personali e dati comportamentali degli utenti, che devono essere dati di qualità, dati recenti e dinamici, e provenire da più fonti per descrivere in modo completo l'ambiente. Se i dati utilizzati per addestrare i modelli di IA sono parziali o incompleti, i modelli stessi possono ereditare questi *bias*, portando a decisioni non accurate e potenzialmente discriminatorie[27]. Modelli di IA addestrati su una determinata area geografia o su uno specifico gruppo di utenti (categorie professionali, gruppi demografici, genere) porteranno a una protezione inadeguata, alla penalizzazione di certi gruppi, a discriminazioni e disuguaglianze[28].

La raccolta e l'analisi massiccia dei dati personali e comportamentali (attività *online*, comunicazioni, comportamenti di utilizzo, dati di localizzazione) rappresentano un rischio significativo per la privacy degli utenti e il diritto alla protezione dei dati personali, creando una tensione tra la necessità di raccogliere informazioni dettagliate per migliorare la sicurezza e i diritti degli individui. Il monitoraggio

[26] Alcuni riferimenti essenziali, F. Pasquale, *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale*, Roma, Luiss University Press, 2021; U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino, 2020; A. D'Aloia (a cura di), *Intelligenza artificiale e diritto: come regolare un mondo nuovo*, Milano, 2020; G. Alpa (a cura di), *L'intelligenza artificiale: il contesto giuridico*, Modena, 2021; P. Benanti, *Human in the loop. Decisioni umane e intelligenze artificiali*, Milano, 2022; A.; J. Searle, *Intelligenza artificiale e pensiero umano: filosofia per un tempo nuovo*, trad. it. A. Condello, Roma, 2023; S. Salardi, Intelligenza artificiale e semantica del cambiamento: una lettura critica, Torino, 2023; Th. Casadei, S. Pietropaoli, *Intelligenza artificiale: l'ultima sfida per il diritto?,* in Th. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, Milano, 2024.

[27] *Inter alia* J. Kleinberg, J. Ludwig, S. Mullainathan, C. R. Sunstein, *Discrimination in the Age of Algorithms*, in *journal of Legal Analysis*, 10, 2018, 1-62; G. Lasagni, G. Contissa, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi*, in Diritto di internet, 4, 619-634; V. Barone, *Le discriminazioni ai tempi dell'intelligenza artificiale: la questione algoritmi*, in *Diritto e tecnologie informatiche*, *op. cit.*

[28] F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *Archivio Penale*, 2, 2023.

continuo e pervasivo dei sistemi e degli utenti, per identificare minacce e anomalie, può trasformare le pratiche di cybersicurezza in strumenti di sorveglianza persistenti e pervasivi. Questo tipo di sorveglianza, che riguarda tanto gli ambiti lavorativi quanto i singoli e la collettività, può erodere le libertà civili e i diritti fondamentali, creando un ambiente in cui gli individui si sentono costantemente osservati e controllati[29].

L'opacità e la complessità dei modelli di IA rappresentano una criticità significativa anche per la governance della cybersicurezza nella misura in cui le soluzioni basate su IA non saranno in grado di giustificare i risultati (dal rilevamento al processo decisionale) e renderli comprensibili all' essere umano. Questo aspetto diventa infatti particolarmente rilevante quando le decisioni automatizzate hanno conseguenze gravi, come la determinazione di minacce, la risposta a incidenti di sicurezza o ancora l'attribuzione di un indice di rischio ai comportamenti degli utenti interni ai sistemi. La comprensione inoltre è strategica per consentire agli operatori, che sono sommersi da decine di migliaia di avvisi di sicurezza al giorno (la maggior parte dei quali falsi positivi), di valutare meglio le potenziali minacce e di ridurre la stanchezza da allarme[30]. Di conseguenza, anche nel settore della cybersicurezza, la sfida di rendere i modelli di IA spiegabili o interpretabili dagli utenti umani è di primaria importanza; conoscibilità e spiegabilità sono il presupposto per garantire che le decisioni automatizzate siano giuste ed equitative[31].

Questi rischi, assieme a vulnerabilità che saranno analizzate nella prossima sezione, sottolineano la necessità di adottare misure di mitigazione come l'uso di tecniche di IA spiegabili, l'implementazione di controlli rigorosi sui dati di addestramento e la combinazione di IA con la supervisione umana per garantire una difesa robusta contro le minacce informatiche.

A tale proposito, è opportuno osservare che i sistemi di IA descritti, indipendentemente dalle diverse funzioni di cybersecurity che implementano, rientrano nella categoria della IA specifica o ristretta[32], come tutte le applicazioni di IA oggi disponibili. Si tratta di strumenti limitati a un singolo compito o gruppo di operazioni, la cui autonomia è ad oggi alquanto ridotta e il controllo umano prevalente. Probabilmente ci saranno progressi nel grado di automazione e nella velocità dei processi, ma difficilmente l'automazione riguarderà l'intero processo di cybersicurezza. Sembra dunque che nessuna so-

[29] A.C. Amato Mangiameli, *Algoritmi e big data*, in *Rivista di Filosofia del Diritto*, 2019, VII, 1, 107-124; F. Lagioia, G. Sartor, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 11/2020, 88 ss., F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* Torino, 2018; F. Faini, Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina, in *Federalismi.it*, 2/2023. G. Ziccardi, *Tecnologie per il potere*, Raffaello Cortina, 2019.

[30] F. Charmet et al., *Explainable artificial intelligence for cybersecurity: a literature survey* in *Ann. Telecommun*. 77, 789–812 (2022); R. Guidotti et al., *A Survey Of Methods For Explaining Black Box Models*, in *ACM Computing Surveys*, LI, 93 (2018), 1-42.

[31] In argomento, M. Palmirani, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in *XXVI lezioni di Diritto dell'Intelligenza artificiale*, Giappichelli, Torino, 2020; Pagallo, *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, 1/2020; E. Longo, *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?,* I, Bologna, 2022, 349 ss.; A. Andronico, Th. Casadei (a cura di), *Algoritmi ed esperienza giuridica*, in *Ars Interpretandi*, 1, 2021, 7-164.

[32] Per la differenza tra AI ristretta e generale si veda G. Sartor, *op cit.*, 16.

luzione di IA sarà in grado di svolgere attività di riposta totalmente non supervisionate sia nella protezione del sistema (correzione automatica delle vulnerabilità) sia nella difesa informatica attiva[33].

4. Vulnerabilità e sicurezza dell'intelligenza artificiale

Come molte altre tecnologie, l'IA è a "doppio uso" il che significa che può essere impiegata per migliorare gli strumenti di contrasto alle minacce per la (*cyber*) sicurezza o anche per scopi dannosi e per ottenere vantaggi competitivi in seguito agli attacchi. Le caratteristiche di efficienza, scalabilità e adattabilità rendono l'IA interessante per diversi tipi di attori (statali e non) e sfruttabile per obiettivi difensivi (*Defensive AI*), offensivi o di altri tipo legati alla sicurezza[34]. Non deve sorprendere dunque che tra i pericoli emergenti per la cybersicurezza venga segnalato proprio l'uso e l'abuso della intelligenza artificiale.

Con l'impiego dell'IA saranno realizzati *cyber* attacchi sempre più sofisticati e complessi[35]. Come per la difesa, gli attacchi colpiscono tutti i livelli del cyberspazio: fisico (dispositivi e apparecchiature), logico (software, protocolli) e semantico (dati, informazioni). Sfruttando le medesime tecniche di cyber intelligence implementate nei sistemi di rilevamento delle minacce, gli aggressori sono in grado di preparare e attuare sofisticati attacchi di ingegneria sociale basati sulle informazioni che le potenziali vittime lasciano nella rete e di creare vettori personalizzati: link, siti web, e-mail persuasive, chat bot convincenti e contenuti manipolati (i *deep fake*) non facilmente identificabili come falsi. Inoltre, grazie all'apprendimento rinforzato le minacce informatiche saranno capaci di eludere il rilevamento, adattarsi ad ambienti mutevoli, scoprire vulnerabilità specifiche, propagarsi e persistere sui sistemi bersaglio. Un *malware* con componenti di IA può essere in grado di offuscare il suo funzionamento nel sistema infettato e rispondere in modo creativo e adattativo ai cambiamenti dell'ambiente e al comportamento degli utenti. La permanenza inosservata sul sistema target consentirà, inoltre, di trovare e classificare contenuti utili per l'esfiltrazione e di individuare nuovi punti di attacco. Gli aggressori potrebbero sfruttare i dati di addestramento per generare una *backdoor* nel sistema software di IA o utilizzare l'IA per determinare quale vulnerabilità vale la pena sfruttare. Scenari in cui l'AI diventa strumento per condurre attacchi cyber si classificano come *Offensive IA*.

I sistemi di IA, inoltre, possono essere vulnerabili a causa di debolezze intrinseche o di meccanismi interdipendenti, ancora non risolti o sconosciuti. Attacchi mirati possono sfruttare le vulnerabilità esistenti nelle librerie software open-source più diffuse (le comunità di IA sono particolarmente aperte in termini di trasferimento della conoscenza) oppure mettere in atto *reverse engineering* del modello addestrato sfruttando interfacce di interrogazione pubblicamente accessibili o ancora sfruttare il *prompt* per riuscire ad ottenere da IA generative informazioni sensibili o illegali. Altri attacchi sono in grado di "avvelenare" i dati di addestramento *(data poisoning)*, in questo caso, si presume che l'attaccante abbia accesso ai dati e sia in grado di alterarli e di introdurre manipolazioni in modo che il sistema, addestrato sui dati avvelenati, esegua elaborazioni o previsioni seguendo gli interessi

[33] M.E. Bonfanti, *Artificial intelligence and the offense–defense balance in cyber security*, in *Cyber Security Politics*, Routledge, 2022, 64-78. Questo tipo di risposta potrebbe essere anche indesiderabile per le conseguenze politiche, legali e strategiche che potrebbe generare.

[34] M. Bonfanti, *op. cit.*, 69 ss.

[35] ENISA, *Artificial Intelligence and Cybersecurity Research*, 2023. *Inter alia*, M. Malatji, A. Tolah, *op. cit.*

dell'attaccante. Gli *attacchi avversari*, invece, colpiscono le reti neurali profonde con input progettati dall'aggressore per essere classificati in modo errato e alterare di conseguenza la previsione del sistema di intelligenza artificiale. Se da un lato l'AI diventa sempre più indispensabile per la gestione delle minacce informatiche, la manipolazione dei sistemi software di AI può compromettere l'efficacia stessa dei sistemi di sicurezza. Tutti gli ultimi scenari descritti sono classificati come *Adversarial AI*.

È difficile peraltro fare una stima a medio-lungo termine del perimetro e dell'impatto delle vulnerabilità dei componenti di IA e questo vale anche per gli strumenti impiegati nell'ambito della difesa della (cyber)sicurezza. Si tratta di innovazioni emergenti, la ricerca e le applicazioni negli ultimi anni hanno compiuto progressi molto rapidi e quindi è ragionevole supporre che molte vulnerabilità siano sconosciute e i potenziali abusi debbano ancora essere esplorati. Le implicazioni per la cybersicurezza in questo campo sono ancora meno prevedibili che in altri contesti.

Oltre ad interrogarsi sui molti modi in cui l'IA può essere sfruttata per la protezione del cyber spazio o sulla sua capacità offensiva, è opportuno riflettere sulle buone pratiche di sicurezza informatica per garantire che le componenti di IA inserite nei sistemi siano integre, affidabili e disponibili.

La sicurezza informatica deve essere una priorità e un requisito per tutti i sistemi di IA, quindi anche per quelli progettati per il contesto della cybersecurity.

La progettazione della sicurezza per l'IA è più complessa rispetto ai tradizionali sistemi di ingegnerizzazione del software perché entrano in gioco molti fattori e le minacce non sono solo tecniche, legali o ambientali, ma anche sociali, come illustrato nella sezione precedente. Diventa auspicabile indirizzare l'uso delle tecnologie di IA verso gli obiettivi benefici della cybersicurezza che ha un effetto diretto sulla capacità di sostenere le libertà individuali, lo Stato di diritto e la democrazia, e prevenire i possibili esiti negativi con adeguate misure politiche, giuridiche e tecnologiche. Promuovere nel contesto della cybersicurezza pratiche eticamente positive nell'uso dell'IA significa garantire che il suo sviluppo e impiego avvengano in un contesto socio-tecnico inclusivo di tecnologie, capacità umane, strutture organizzative e norme etiche e giuridiche, in cui siano rispettati e promossi gli interessi individuali e i valori sociali[36].

Metodologie e linee guida per la cybersicurezza delle soluzioni di IA sono ancora in fase di studio[37]. I framework esistenti mirano a promuovere la diffusione di un'intelligenza artificiale affidabile grazie a tre fattori essenziali: (1) rispetto dell'articolato quadro normativo in materia; (2) garanzia dei principi e dei valori etici; (3) solidità dei sistemi AI da un punto di vista tecnico e sociale. La robustezza tecnica e la sicurezza del sistema – robustezza nel caso di problemi e resilienza contro i tentativi di alterare l'uso o le prestazioni – costituiscono, insieme, uno dei sette requisiti fondamentali delle linee guida etiche per una IA "degna di fiducia" (*trustworthy* AI) elaborati dal High-Level Expert Group on Artificial Intelligence nel 2019[38].

[36] Per un'ampia introduzione e discussione si veda L. FLORIDI, *Etica dell'artificiale. Sviluppi, opportunità, sfide*, Milano, 2022. Su etica e intelligenza artificiale, tra gli altri: F. FOSSA, V. SCHIAFFONATI, G. TAMBURRINI (a cura di), *Automi e persone. Introduzione all'etica dell'intelligenza artificiale e della robotica*, Roma, 2021; M. ZANICHELLI, *L'intelligenza artificiale e la persona: tra dilemmi etici e necessità di regolazione giuridica*, in *Teoria e Critica della Regolazione Sociale*, 2, 2021, 141-159; F.H. LLANO-ALONSO, *L'etica dell'intelligenza artificiale nel quadro giuridico dell'Unione europea*, in *Ragion pratica*, 2, 2021, 327-348.

[37] ENISA, Mind the Gap in Standardisation of Cybersecurity for Artificial Intelligence, 2023.

Sotto il profilo giuridico, la cybersicurezza dell'IA, assieme alla accuratezza e alla robustezza, è affrontata dalla nuova legge sulla intelligenza artificiale (Regolamento (UE) 1689/2024, c.d. AI Act) all'articolo 15. Ai considerando 75 e 76, il legislatore sottolinea che la robustezza tecnica è un elemento cruciale perché i sistemi di IA ad alto rischio siano in grado di resistere a comportamenti dannosi o indesiderati che possono emergere a causa di errori, guasti, o situazioni impreviste e, parimenti, la sicurezza informatica è fondamentale per proteggere i sistemi di IA dai tentativi di attacco da parte di aggressori che mirano a sfruttare le vulnerabilità del sistema. I requisiti di cybersicurezza stabiliti dall'AI Act contemplano quattro elementi principali[39]: (1) i sistemi di intelligenza artificiale ad alto rischio devono essere garantiti e progettati per essere resilienti ai tentativi di alterarne l'uso, il comportamento e le prestazioni e di comprometterne le proprietà di sicurezza da parte di terzi malintenzionati che ne sfruttano le vulnerabilità; (2) per raggiungere questi obiettivi devono essere implementate misure organizzative e tecniche; (3) per i sistemi di IA ad alto rischio deve essere effettuata una valutazione del rischio di cybersecurity e, infine, (4) le soluzioni tecniche devono essere adeguate alle circostanze e ai rischi pertinenti.

Dopo l'entrata in vigore della legge sull'IA, tutti i sistemi di IA ad alto rischio definiti dalla legislazione dovranno essere sottoposti a una valutazione di conformità e rispettare i requisiti di cybersicurezza prima di poter essere utilizzati o messi in servizio nel mercato dell'UE.

Le disposizioni in materia di cybersicurezza introdotte dalla legge sulla intelligenza artificiale si inseriscono nel complesso quadro legislativo europeo sulla cybersicurezza, introdotto nella prima sezione, rendendo dunque necessario il coordinamento tra i diversi perimetri normativi. In particolare, per i sistemi di IA ad alto rischio che rientrano anche nell'ambito di applicazione del cd. Cyber Resilience Act (CRA), regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali – e quindi suscettibile di ricomprendere nel suo ambito di applicazione anche sistemi di IA –, il legislatore europeo ha previsto che tali sistemi debbano essere conformi ai requisiti essenziali di cui all'allegato I del CRA[40].

Per garantire la conformità ai requisiti legislativi, vi è un forte indirizzamento da parte della Commissione europea verso l'adesione a standard tecnici armonizzati. Ciò anticipa la necessità di un continuo processo di standardizzazione sulla cybersicurezza dell'IA nei prossimi anni. La gestione della cybersicurezza può avvalersi di standard tecnici e pratiche consolidate che comprendono procedure sui principi organizzativi, sulla gestione del rischio e misure di sicurezza; tuttavia, gli standard esistenti non sono ancora stati estesi alle specificità degli scenari IA.

Sul punto, il *Multilayer framework for Good cybersecurity practices for AI* di ENISA (2023) suggerisce di progettare la sicurezza in tre livelli: al primo livello (*Cybersecurity Foundations*), l'insieme di conoscenze e pratiche di base della cybersecurity che devono essere applicate a tutti gli ambienti ICT,

[38] I-HLEG, High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, 2019.

[39] European Commission, Joint Research Centre, H. JUNKLEWITZ, et al., *Cybersecurity of artificial intelligence in the AI Act – Guiding principles to address the cybersecurity requirement for high-risk AI systems*, Publications Office of the European Union, 2023.

[40] P.G. CHIARA, *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in *Rivista Italiana di Informatica e Diritto*, 1, 2023, 143-153.

compresi quelli che ospitano i sistemi di IA; al secondo livello (*AI specific),* le pratiche di cybersecurity necessarie per affrontare le specificità dei componenti dell'IA con una visione del loro ciclo di vita, delle loro proprietà, delle minacce e dei controlli di sicurezza che sarebbero applicabili indipendentemente dal settore; al terzo livello (*Sectorial AI*), le diverse *best practices* che possono essere utilizzate dagli stakeholder settoriali per proteggere i loro sistemi di IA. In questo livello dovrebbero collocarsi i sistemi di IA ad alto rischio, come identificati dalla legge sull'IA.

5. Conclusioni

Alla luce di quanto presentato, l'intelligenza artificiale rappresenta un potente strumento per migliorare la protezione contro le minacce informatiche. Guardando al futuro, l'IA consentirà lo sviluppo di sistemi di difesa proattivi e adattativi, capaci di evolversi e adattarsi continuamente in risposta alle nuove minacce, e favorirà una maggiore collaborazione e condivisione delle informazioni tra settore pubblico e privato, migliorando la resilienza complessiva. L'IA introduce anche importanti sfide alla cybersicurezza: dalla maggior capacità offensiva da parte di attori malevoli a problemi specifici – quali il rischio di iniquità e discriminazioni e la profilazione – e a nuove e inedite vulnerabilità legate all'incertezza dell'innovazione. Sullo sfondo, è opportuno ricordare come l'adozione sempre più pervasiva di queste tecnologie di sicurezza solleva – paradossalmente – preoccupazioni circa la normalizzazione della sorveglianza: per essere efficienti ed efficaci, le tecnologie di cybersicurezza analizzate nel presente contributo, soprattutto se combinate con sistemi di intelligenza artificiale, devono trattare una vasta mole di dati, anche personali, potenzialmente compromettendo il diritto alla protezione dei dati e alla privacy.

I sistemi per il rilevamento di anomalie, in particolare, svolgono un monitoraggio continuo del traffico di rete, dei comportamenti degli utenti e dei processi per identificare, con l'aiuto di algoritmi di apprendimento automatico, deviazioni rispetto al comportamento normale del sistema o dell'utente. Questo approccio, essenziale per la cybersicurezza, perché aiuta le organizzazioni a rispondere in tempo reale a minacce esterne e interne, evidenzia come la sicurezza informatica possa diventare una giustificazione per la sorveglianza, in diversi contesti.

La proposta di Regolamento di attuazione della direttiva NIS 2 (UE) 2022/2555 pubblicata dalla Commissione europea il 27 giugno 2024, che stabilisce norme per l'applicazione della direttiva con riguardo ai requisiti tecnici e metodologici delle misure di gestione del rischio di cibersicurezza[41], inserisce le tecnologie di rilevamento delle anomalie nelle pratiche di cybersicurezza obbligatorie per un serie di soggetti e ne incentiva l'uso in tutti gli Stati membri. Non vengono fornite, tuttavia, indicazioni su come queste tecnologie debbano essere impiegate in modo da rispettare i diritti fondamentali alla protezione dei dati e alla privacy della Carta dei Diritti fondamentali dell'Unione europea.

La possibilità di trarre reale beneficio dalle tecnologie emergenti, per garantire un futuro digitale più sicuro, giusto e resiliente, dipenderà non solo dalla capacità delle organizzazioni sia pubbliche che private di fare progressi nelle ricerche su IA e cybersicurezza, nella loro applicazione e nello sviluppo delle competenze, ma anche dallo studio critico continuo degli impatti di queste tecnologie sulle sfe-

[41] Cfr. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en.

re giuridiche dei cittadini e, pertanto, dalla risposta legislativa che deve essere proporzionata e adeguata. L'approccio tecnico-ingegneristico negli ambienti complessi di oggi non è sufficiente ma occorre sviluppare una visione olistica di controllo del rischio che comporti la protezione in modo coordinato dei molti valori in gioco e che diventi anche un requisito etico e giuridico alla base dello sviluppo dei sistemi informatici.

ISSN 2284-4503