https://doi.org/10.60923/issn.1825-1927/22648 ISSN 1825-1927

Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone

Gianluigi Fioriglio [1]

[1] Università di Modena e Reggio Emilia

Abstract: Il contributo discute le principali questioni di cibersicurezza dei sistemi di Intelligenza Artificiale (IA) in una prospettiva informatico-giuridica. Premesso un succinto inquadramento normativo anche su concetti basilari della sicurezza informatica, vengono dapprima analizzate le principali minacce che incombono attualmente sui sistemi informatici e di IA, tenendo conto che quest'ultimi sono *anche* sistemi informatici. Viene poi discussa la vulnerabilità degli agenti artificiali e umani nella Società algoritmica, delineandone criticità e possibili evoluzioni.

Keywords: intelligenza artificiale, cibersicurezza, minaccia informatica, Società algoritmica, vulnerabilità.

1 Introduzione[1]

Com'è noto, l'intelligenza artificiale (di seguito solo "IA") sta progressivamente e rapidamente caratterizzando la società contemporanea[2]. Da un lato, ciò comporta numerose questioni etiche e giuridiche[3], ben preconiz-

gianluigi.fioriglio@unimore.it (Gianluigi Fioriglio);

1. Il presente contributo prosegue alcune riflessioni sviluppate nell'ambito dell'Officina Informatica DET "Diritto Etica e Tecnologia", istituita presso il CRID – Centro di Ricerca Interdipartimentale su Discriminazione e vulnerabilità dell'Università di Modena e Reggio Emilia (diretto da Thomas Casadei e da lui fondato con Gianfrancesco Zanetti). Ringrazio i colleghi e le colleghe nonché le giovani studiose e i giovani studiosi del CRID per le numerose occasioni di confronto. Ringrazio, infine, i referee anonimi per le preziose osservazioni, che hanno contribuito ad accrescere il rigore scientifico e la qualità complessiva del contributo.

2. Per un autorevole inquadramento tecnico sull'IA cfr. S. Russell – P. Norvig, *Artificial Intelligence: A Modern Approach*, *Global Edition*, Pearson, Harlow, 4th edition, 2022.

3. Cfr., fra gli altri: S. Amato, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020; T. Casadei-S. Pietropaoli, *Intelligenza artificiale: l'ultima sfida per il diritto?*, in Id. (a cura di), *Diritto e tecnologie informatiche*. *Seconda edizione aggiornata e ampliata*. *Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 259-274; G. Contissa, *Information Techonology for the Law*, Giappichelli, Torino, 2017; L.A. Dimatteo – C. Poncibò – M. Cannarsa (edited by), *The Cambridge handbook of artificial intelligence. Global perspectives on law and ethics*, Cambridge University Press, Cambridge, 2022; F. Donati – G. Finocchiaro – F. Paolucci – O. Pollicino (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè Francis Lefebvre, Milano, 2025; G. Finocchiaro, *Diritto dell'intelligenza artificiale*, Zanichelli, Bologna, 2024; L. Floridi, *Etica dell'intelligenza artificiale, sviluppi, opportunità, sfide*, Raffaele Cortina, Milano, 2022; B. Indovina, *Informatica, diritto, intelligenza artificiale*, EGEA, Milano, 2024; F.H. Llano Alonso, *Homo ex machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnòlogica*, Tirant lo Blanch, Valencia, 2024; L. Palazzani, *Etica della regolazione dell'intelligenza artificiale*, in *Rivista di filosofia del diritto.*, 2025, 1, pp. 9-20; L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale*. *Sfide etiche al diritto*, Studium, Roma, 2020; F. Romeo, *Il diritto artificiale*, Giappichelli, Torino, 2002; P. Moro – C. Sarra (a cura di), *Tecnodiritto*. *Temi e problemi di informatica e robotica giuridica*, FrancoAngeli, Milano, 2017; S. Salardi, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, Giappichelli, Torino, 2022; G. Sartor, *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022.

Copyright © 2025 Gianluigi Fioriglio
This work is licensed under the Creative Commons BY License.
https://creativecommons.org/licenses/by/4.0/

zate dall'informatica giuridica[4]; dall'altro, implica che la cibersicurezza dell'IA (in senso lato, come meglio precisato nel prosieguo) sia assolutamente fondamentale. Se, infatti, oggi si registra un impiego sempre più diffuso di sistemi di IA in ambiti molteplici ed eterogenei, non v'è dubbio che la società stessa si trovi a dipendere dalla seconda in modo più o meno forte, e che l'IA, a sua volta, debba essere anche "sicura" per funzionare correttamente. Del resto, non garantire la sicurezza dei sistemi di IA la porterebbe a essere un moderno e sofisticato gigante dai piedi d'argilla; come non c'è privacy senza sicurezza, non c'è IA senza sicurezza.

Il presente contributo è dunque finalizzato a: (i) introdurre succintamente il quadro normativo vigente e i concetti basilari della sicurezza informatica; (ii) analizzare le minacce informatiche dei sistemi informatici e dei sistemi (e dei modelli) di IA; (iii) riflettere sulla vulnerabilità degli agenti artificiali e umani nella società algoritmica, che – può già anticiparsi – ha un ambito ancor più ampio di quello connesso alla sola cibersicurezza.

Prima di introdurre talune nozioni fondamentali, è opportuno riportare una semplice e generale definizione di "sicurezza": "la condizione che rende e fa sentire di essere esente da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli, e simili"[5]. Essa, in tutta evidenza, risulta applicabile anche all'ambito informatico, fermo restando che debba essere compiutamente dettagliata e che tale ambito è tutt'altro che isolato dagli altri: si pensi al lavoro, all'ambiente, alla circolazione stradale, e così via. Questi e altri settori, infatti, sono pervasi in modo più o meno marcato dall'informatica e dall'IA, per cui le conseguenze di eventuali problematiche di cibersicurezza sono, in linea di principio, idonee a riverberarsi sugli stessi. A titolo esemplificativo, si pensi alle minacce che, provocando il malfunzionamento di macchinari o dispositivi "intelligenti" (e non), potrebbero ferire o uccidere lavoratori e lavoratrici, danneggiare l'ambiente, provocare sinistri stradali.

Può, del resto, darsi oramai per acquisito che la società sia sempre più "algoritmica"[6] e che l'IA sia un "meccanismo di amplificazione del potere"[7], in quanto dati, di qualsiasi tipologia e in qualsiasi formato, vengono elaborati in modo sempre più automatizzato e "intelligente", con organizzazione dei processi decisionali, e delega totale o parziale del loro svolgimento, a *software* che – nell'esecuzione di algoritmi più o meno complessi e interconnessi – elaborano le informazioni, giungendo anche ad apprendere dalle stesse grazie agli algoritmi di *machine learning* (apprendimento automatico) che vengono implementati.

Il quadro "tecnologico" e di mercato si evolve incessantemente (così come le minacce informatiche), mentre quello normativo, a livello europeo, si sta più lentamente delineando anche per ciò che concerne la cibersicurezza nell'ambito di tre macroaree di intervento (resilienza, contrasto alla criminalità informatica, ciberdifesa e ciberdiplomazia); sono state, infatti, gradualmente adottate o proposte diverse normative che definiscono un nuovo assetto giuridico in materia di cibersicurezza[8], concretizzando – da ultimo – la relativa

4. Sull'evoluzione dell'informatica giuridica in Italia cfr. G. Peruginelli – M. Ragona (a cura di), *L'informatica giuridica in Italia*, Edizioni Scientifiche Italiane, Napoli, 2014; per una ricostruzione dell'evoluzione dell'informatica giuridica a livello internazionale cfr. altresì G. Fioriglio, *Temi di informatica giuridica*, Aracne, Roma, 2004; M.G. Losano, *Scritti di informatica e diritto. Per una storia dell'informatica giuridica* (a cura di P. Garbarino-M. Cavino), Mimesis, Milano, 2022 (2 voll.). Doveroso, altresì, menzionare "Cibernetica, diritto e società" di Vittorio Frosini che, come ricordato da Giovanni Sartor nell'introduzione alla versione digitale recentemente pubblicata (collana "La memoria del diritto" curata da L. Loschiavo, G. Pino, V. Zeno-Zencovich), "è stato il primo volume di informatica giuridica nel nostro paese (poco dopo, nel 1969, sarà la volta di"Giuscibernetica: Macchine e modelli cibernetici nel diritto", di Mario Losano)(V. Frosini, *Cibernetica, diritto e società*, Roma Tre Press, Roma, (1968) 2023, disponibile online: https://romatrepress.uniroma3.it/wp-content/uploads/2023/09/cibe-vifr.pdf).

5. Cfr. Enciclopedia Treccani, https://www.treccani.it/enciclopedia/sicurezza/.

6. Sulla Società algoritmica, e sulle diverse problematicità che quest'ultima comporta, la letteratura scientifica è assai vasta; cfr., *ex multis*, J. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal*, Vol. 78, 5, 2017, pp. 1217-1241; F. Pasquale, *Towards a Fourth Law of Robotics: Preserving Attribution, Responsability and Explanaibility in an Algorithmic Society*, in *Ohio State Law Journal*, 2017, 78, pp. 1243-1255; G. Gorgoni, *Stay Human. The quest for Responsability in the Algorithmic Sociey*, in *JELT - Journal of Ethics and Legal Technologies*, 2020, 2, pp. 31-47; W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithmics*, Cambridge University Press, Cambridge, 2020; M. Schuilenburg – R. Peeters (ed.), *The Algorithmic Society. Technology, Power and Knowledge*, Routledge, London, 2021; H.W. Micklitz – O. Pollicino – A. Simoncini – G. Sartor – G. De Gregorio (ed.), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021; G. Fioriglio, *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici,* in *Ars interpretandi*, 2021, 1, pp. 53-67.

7. L. Corso, *Legge dell'algoritmo e rule of law. Riflessioni preliminari*, in *PasSaggi costituzionali*, 2024, 1, p. 210.

8. R. Brighi, *Cybersicurezza e intelligenza artificiale. Un'analisi critica*, in *BioLaw Journal*, 2024, 1 (special issue), p. 111.

strategia dell'UE "per il decennio digitale"[9].

Ad oggi, si registrano diverse normative che assumono rilevanza e possono qui ricordarsi, senza pretesa di esaustività: la direttiva NIS2 sulle misure per un livello comune elevato di cibersicurezza (Direttiva (UE) 2022/2555, recepita in Italia con il d.lgs. 138/2024); il GDPR sulla protezione dei dati personali (Regolamento (UE) 2016/679); il regolamento DORA sulla resilienza operativa digitale per il settore finanziario (Regolamento (UE) 2022/2554); il "*Cybersecurity Act*", per l'appunto, sulla cibersicurezza (Regolamento (UE) 2019/881); il "*Cyber Resilience Act*" sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (Regolamento (UE) 2024/2487); l'*AI Act*, ovviamente, sull'IA (Regolamento (UE) n. 2024/1689).

È altresì doveroso menzionare la creazione di istituzioni finalizzate proprio al rafforzamento della cibersicurezza, che è sempre più strategica per ciascuno stato. Così, a livello europeo bisogna ricordare l'Agenzia dell'Unione europea per la cibersicurezza (ENISA, *European Union Agency for Network and Information Society*) e, a livello italiano, l'Agenzia per la Cibersicurezza Nazionale (ACN).

In particolare, l'ENISA è stata istituita con il Regolamento (CE) n. 460/2004 e inizialmente denominata "Agenzia europea per la sicurezza delle reti e dell'informazione" (ossia ENISA, "European Network and Information Security Agency", acronimo tuttora mantenuto nonostante il Cyber Security Act ne abbia mutato la denominazione in Agenzia dell'Unione europea per la cibersicurezza – *European Union Agency for Cybersecurity*). Essa ha il compito di rafforzare la sicurezza informatica nell'UE, supportando gli Stati membri nella protezione di reti, sistemi e dati dalle minacce informatiche. Fra l'altro, presta consulenza strategica, elabora linee guida nel proprio ambito di competenza e coordina esercitazioni di cibersicurezza allo scopo di migliorare la resilienza dei sistemi informatici dell'UE dinanzi agli attacchi informatici.

L'ACN, istituita con il d.l. n. 82/2021, ha il compito principale di garantire la sicurezza delle infrastrutture critiche, prevenendo e contrastando le minacce informatiche. Coordina la risposta a incidenti informatici, supporta aziende e istituzioni nel migliorare la sicurezza dei loro sistemi e promuove la cultura della cibersicurezza attraverso formazione e sensibilizzazione, collabora con altre istituzioni a livello internazionale per affrontare le sfide globali legate alla sicurezza digitale.

Prima di approfondire i profili di cui si è detto, è opportuno premettere taluni concetti chiave, a partire dalla definizione di cibersicurezza di cui all'art. 2(1) del Regolamento (UE) 2019/881: "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"[10]. Per "minaccia informatica" può invece intendersi "qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone" (Art. 2(8) Regolamento (UE) 2019/881); essa è "significativa", quando, in base alle relative caratteristiche tecniche, "si presume possa avere un grave impatto sui sistemi informatici e di rete di un soggetto o degli utenti di tali servizi del soggetto causando perdite materiali o immateriali considerevoli" (art. 6(11) Direttiva NIS2).

Sempre nella Direttiva NIS2 si possono reperire ulteriori definizioni di particolare rilevanza: l' "incidente", ossia "un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi" (art. 6(6)). L'incidente può essere "su vasta scala" se "causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri" (art. 6(7))[11].

9. Cfr., in particolare, la *Comunicazione congiunta al Parlamento europeo e al Consiglio, La strategia dell'UE in materia di cibersicurezza per il decennio digitale* del 16 novembre 2020 e la *Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale* del 23 giugno 2021.

10. Come rilevato dall'ENISA, "la cibersicurezza copre tutti gli aspetti della prevenzione, previsione, tolleranza, rilevamento, mitigazione, rimozione, analisi e investigazione degli incidenti informatici. Considerando i diversi tipi di componenti del cyberspazio, la cybersicurezza dovrebbe includere i seguenti attributi: disponibilità, affidabilità, sicurezza, riservatezza, integrità, manutenibilità (per sistemi tangibili, informazioni e reti); robustezza, sopravvivenza, resilienza (per supportare la dinamicità del cyberspazio); responsabilità, autenticità e non ripudio (per garantire la sicurezza delle informazioni)" (ENISA, *ENISA overview of cybersecurity and related terminology*, Heraklion, 2017, p. 6).

11. Può aversi anche un "quasi incidente", ossia un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato» (art. 6(5)).

In tutta evidenza, le definizioni di minaccia informatica e di incidente rendono palese come gli accadimenti che danneggiano, perturbano o hanno un impatto negativo sui sistemi informativi e sulle reti possano ben essere "non informatici", come un incendio, un furto, un terremoto, e così via.

Infine, il rischio[12] è "la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi" (art. 6(9)).

Ebbene, le succinte definizioni richiamate (in particolare quelle di minaccia, incidente e rischio) evidenziano come la dimensione tecnico-operativa della cibersicurezza si intrecci inevitabilmente con profili che interessano l'ordinamento giuridico nel suo complesso. La cibersicurezza protegge l'integrità della società, il cui buon funzionamento dipende oggi, in misura crescente, da quello delle tecnologie; pertanto non è sufficiente limitarsi alla mera descrizione degli eventi dannosi o alla stima della probabilità di accadimento: occorre interrogarsi sul ruolo che il diritto deve assumere di fronte a tali vulnerabilità. Con specifico riferimento alle vulnerabilità dei sistemi di intelligenza artificiale, la prospettiva esclusivamente descrittiva risulta insufficiente per affrontare la questione centrale della funzione giuridica nell'ecosistema digitale. In tale prospettiva, la metodologia dell'informatica giuridica – come elaborata dalla cosiddetta scuola svedese e, in particolare, nei contributi di Peter Seipel[13] – indica l'adozione di un modello proattivo di regolazione: non solo una reazione agli incidenti, ma un ruolo anticipatorio del diritto, orientato da principi operativi quali la sicurezza sin dalla progettazione (*security by design*) e l'*accountability*.

Tali principi informano già il quadro normativo europeo (cfr., in particolare, il GDPR e l'AI Act) e non devono restare enunciati formali: essi sono riconducibili a obblighi concreti – a titolo esemplificativo, analisi e gestione continue del rischio, data governance, documentazione tecnica, audit e valutazioni di conformità – e possono, se opportunamente interpretati, costituire categorie giuridiche operative idonee a vincolare sviluppatori, enti pubblici e imprese nella fase di concezione, sviluppo e implementazione degli algoritmi. La prospettiva informatico-giuridica, dunque, non si limita a recepire le "tradizionali" vulnerabilità dei sistemi informatici, ma le trasforma in parametri giuridici operativi, contribuendo a rafforzare la resilienza dell'ecosistema digitale.

12. In linea più generale, può osservarsi come l'approccio basato sul rischio caratterizzi diverse normative a livello europeo, nel tentativo di regolamentare i rischi aumentando *l'accountability degli* attori pubblici e privati in relazione ai rischi e agli effetti collaterali potenziali derivanti dalle loro attività. L'emergere di questo approccio nelle politiche digitali europee è particolarmente evidente nei recenti sviluppi normativi in materia di dati (GDPR), contenuti online (*Digital Services Act*, ossia il Regolamento (UE) 2022/20265), intelligenza artificiale (*AI Act*), con un approccio rispettivamente *bottom-up* (la valutazione del rischio e le misure di mitigazione sono lasciate primariamente ai titolari e ai responsabili), misto (identifica in modo *top-down* quattro categorie di rischio per i fornitori di servizi di intermediazione, lasciando discrezionalità nella scelta delle misure da adottare), *top-down* (identifica le varie categorie di rischio e impone obblighi differenziati)(G. De Gregorio – P. Dunn, *The European risk-based approaches: connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, 59, 476-477).

13. Utili spunti possono giungere dalla scuola svedese di informatica giuridica e dall'opera di Peter Seipel; basti qui ricordare quanto affermato in merito a una visione caleidoscopica della ICT Law: "ICT can and should be seen as a social engine with capacity to generate and/or support far-reaching changes in society. Traditionalists are slow to accept this whereas renewers see opportunities to develop ICT law so as to improve democracy, conditions of life, access to knowledge etc. Efforts of this kind presuppose an ability to deal with social change and to be aware of the importance of a sound information infrastructure in society. Among other things, the idea of ICT as a surveillance technology must be balanced against other ideas of technology, not least the idea of ICT as a survival technology. On the whole, how one sees ICT law – as a matter of business as usual or as a matter of renewal – depends perhaps more on one's understanding of ICT than on one's understanding or jurisprudence. Or, why not: it depends on understanding ICT as jurisprudence" (P. Seipel, *ICT Law – A Kaleidoscope View*, in *Scandinavian Studies in Law – ICT Legal Issues*, 2010, p. 56).

2 La sicurezza dei sistemi informatici

In linea generale, i sistemi di IA sono anche sistemi informatici e, per ciò che concerne i profili di sicurezza[14], bisogna tener conto di questa duplice natura. In ragione di tale presupposto, si deve quindi prima analizzare la sicurezza informatica in termini generali per poi analizzarne le peculiarità.

"Tradizionalmente", a un alto livello di astrazione che comprende il profilo tecnico e quello amministrativo, la sicurezza informatica si estrinseca in tre categorie di misure (o controlli), che toccano, rispettivamente, i profili della robustezza, della resilienza e della risposta dei sistemi. Ciò comporta la previsione e l'implementazione di misure: (i) finalizzate a prevenire un incidente informatico impedendo così la manifestazione del rischio (proteggendo il sistema dagli attacchi previo controllo dei punti di vulnerabilità del sistema; (ii) di monitoraggio degli eventi avversi, così da poter rilevare gli incidenti di sicurezza e le relative conseguenze, e agire di conseguenza; (iii) di ripristino che, in risposta all'evento, permettano la minimizzazione dei danni con la riattivazione tempestiva del sistema e delle sue funzionalità, senza perdita di dati. Questi ambiti includono diversi strumenti tecnici e misure organizzative: dal controllo degli accessi al *disaster recovery*, dalla crittografia ad hardware e software per la difesa perimetrale, dai sistemi di rilevamento delle intrusioni alle misure di sicurezza fisica, e così via[15].

La c.d. triade CIA riassume i tre principi chiave della sicurezza informatica: *confidentiality* (confidenzialità o riservatezza), *integrity* (integrità), *availability* (disponibilità). Più specificatamente, (i) la confidenzialità è relativa al rispetto delle restrizioni sull'accesso e sulla divulgazione delle informazioni, in tutto il loro ciclo di vita; (ii) l'integrità indica la protezione delle informazioni da modifiche o cancellazioni non autorizzate nonché la garanzia di non ripudiabilità e di autenticità dei dati stessi; (iii) la disponibilità concerne l'accesso tempestivo e affidabile alle informazioni, oltre alla loro fruibilità in modo continuativo ed efficiente.

Quanto sin qui esposto non deve tuttavia far ritenere che la sicurezza informatica sia una questione meramente "tecnico-ingegneristica"[16]. Richiede, invece, un approccio olistico che, tenendo conto delle peculiarità settoriali e della dimensione transnazionale delle minacce, integri profili tecnologici, fattori umani e governance strategico-politica. La cybersecurity esige, fra l'altro, il contributo di giuristi, specialisti della comunicazione, psicologi e analisti economici, al fine di affrontarne in modo coordinato le implicazioni giuridiche, reputazionali, comportamentali ed economiche[17].

Ciò appare ancor più chiaro ove si prenda in considerazione la schematizzazione operata dall'ENISA adottando il modello della Piramide di Maslow; essa illustra una possibile organizzazione gerarchica degli strati di protezione della cibersicurezza: (i) *protezione della democrazia e dei diritti umani*: etica informatica, ciberdemocrazia, diritti umani nel cyberspazio, valori fondamentali dell'UE; (ii) *protezione della stabilità globale*: norme informatiche, diplomazia informatica, difesa informatica, guerra informatica; (iii) *protezione*

14. Sulla sicurezza informatica cfr., *ex multis*: S. Aterno, *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, Pisa, 2022; F. Casarosa – G. Comandé, *Aspettando la NIS2: ovvero il diritto privato della Cybersecurity*, in *Il Diritto dell'informazione e dell'Informatica*, 2024, 1, pp. 29-53; P. Cornish, *The Oxford Handbook of Cyber Security*, Oxford University Press, Oxford, 2022; G. D'Angelo – G. Giacomello, *Cybersicurezza. Che cos'è e come funziona*, Il Mulino, Bologna, 2023; T.F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni Costituzionali*, 2024, 2, pp. 277-304; E. Longo, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna parlamentare*, 2024, 2, pp. 313-347; F.P. Micozzi, *Sicurezza informatica. Obblighi e responsabilità dopo il recepimento della NIS2 e la l. n. 90/2024*, Wolters Kluwer, Milano, 2024; L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, 14, 2024, pp. 179-197; S. Pietropaoli, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Giappichelli, Torino, II ed., 2025; M. Pietrangelo, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista italiana di informatica e diritto*, 2024, 2, pp. 14-24; M.G. Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technlogy Analysis*, Bloomsbury, London, 2023; A. Segura – Serrano (ed.), *Global Cybersecurity and International Law*, Taylor-Francis, New York and London, 2024; E: Sorrentino – A.F. Spagnuolo, *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in *Rivista italiana di informatica e diritto*, 2024, 2, 685-701; R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Franco Angeli, Milano, 2023; A. Venanzoni, *L'ordine costituzionale della cybersecurity, in Forum di Quaderni Costituzionali*, 2024, 4, pp. 33-80; G. Ziccardi, *Dati avvelenati. Truffe, virus informatici e falso online*, Raffaello Cortina, Milano, 2024.

15. P.G. Chiara-R. Brighi, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 21, 2021, p. 19.

16. R. Brighi, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in T. Casadei – S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, cit., p. 77.

17. F.P. Micozzi, *Sicurezza informatica. Obblighi e responsabilità dopo il recepimento della NIS2 e la L. n. 90/2024*, cit., p. 2.

del mercato unico digitale: attacchi informatici, crimine informatico, spionaggio informatico, sabotaggio informatico; (iv) *protezione degli asset critici*: Direttiva NIS (oggi NIS2) e sugli operatori di servizi essenziali (OES); (v) *protezione di base della sicurezza*: igiene informatica; sicurezza e protezione degli utenti del cyberspazio (Internet)[18].

Prendendo come riferimento quanto osservato proprio da ENISA nel suo rapporto annuale sulla cibersicurezza[19], può osservarsi che le principali minacce sono oggi costituite da:

a) *ransomware*, quando gli attaccanti ottengono l'accesso non autorizzato alle risorse di un obiettivo, come dati, sistemi o reti, e chiedono un riscatto per ripristinare l'accesso a queste risorse o minacciano di esporre pubblicamente o distruggere permanentemente i dati sensibili. Questi attacchi possono comportare diverse forme di estorsione, non solo con l'obiettivo di ottenere un guadagno finanziario, ma anche sfruttando la minaccia di danni alla reputazione, interruzione operativa o esposizione di informazioni riservate per raggiungere gli obiettivi degli attaccanti [20],

b) *malware*, noto anche come codice maligno o logica maligna: un termine generico utilizzato per descrivere qualsiasi software o firmware progettato per eseguire un processo non autorizzato che avrà un impatto negativo sulla riservatezza, integrità o disponibilità di un sistema [21],

c) ingegneria sociale, che comprende una vasta gamma di attività che sfruttano l'errore o il comportamento umano per ottenere l'accesso a informazioni o servizi. Utilizza varie forme di manipolazione per ingannare le vittime e indurle a commettere errori o a cedere informazioni sensibili o riservate. Gli utenti possono essere indotti ad aprire documenti, file o e-mail, a visitare siti web o a concedere l'accesso a sistemi o servizi. Questa tipologia di minaccia comprende principalmente i seguenti vettori di attacco: *phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps* e *scareware*. Sebbene le tecniche di ingegneria sociale siano spesso utilizzate per ottenere l'accesso iniziale, possono anche essere utilizzate in fasi successive di un incidente o violazione. Fra gli esempi rilevanti possono citarsi la compromissione dell'e-mail aziendale, la frode, la sostituzione di persona, la falsificazione e, più recentemente, l'estorsione[22],

d) violazioni dei dati (personali e non). In una prospettiva tecnica, le minacce contro i dati possono essere ampiamente classificate come violazione dei dati (*data breach*) o fuga di dati (*data leak*). Sebbene vengano spesso utilizzate in modo intercambiabile, implicano concetti fondamentalmente diversi che riguardano principalmente il modo in cui si verificano. La violazione dei dati è un attacco informatico intenzionale compiuto da un criminale informatico con l'obiettivo di ottenere accesso non autorizzato e rilasciare dati sensibili, riservati o protetti. In altre parole, una violazione dei dati è un attacco deliberato contro un sistema o un'organizzazione con l'intenzione di entrare in possesso di dati. La fuga di dati è un evento (come configurazioni errate, vulnerabilità o errori umani) che può causare la perdita o l'esposizione non intenzionale di dati sensibili, riservati o protetti (gli attacchi intenzionali sono talvolta indicati come *data exposure*)[23];

e) *Denial of Service - DoS* (negazione del servizio), anche distribuita (*DDoS*). Gli attacchi DDoS minano la disponibilità di sistemi e dati, per cui gli utenti di un sistema o servizio non sono in grado di accedere ai dati, ai servizi o ad altre risorse rilevanti. Ciò può essere ottenuto esaurendo il servizio e le sue risorse o sovraccaricando i componenti dell'infrastruttura di rete. L'impatto degli attacchi DDoS è spesso limitato e simbolico[24];

18. ENISA, *ENISA overview of cybersecurity and related terminology*, Heraklion, 2017, 4.

19. ENISA, *ENISA threat landscape 2024*, Attiki-Heraklion-Brussels, 2024, 7-8.

20. Ivi, p. 7.

21. *Ibidem*.

22. Ivi, pp. 7-8.

23. Ivi, p. 8.

24. *Ibidem*.

f) manipolazione delle informazioni, ossia una condotta per lo più lecita che minaccia o può influire negativamente su valori, procedure e processi politici. Tale attività è di natura manipolativa, condotta in modo intenzionale e coordinato. Può essere attuato da attori statali o non statali, inclusi propri agenti all'interno e all'esterno del loro territorio[25].

È bene precisare che determinati attacchi informatici possono provocare la violazione di dati personali ai sensi del GDPR (ossia la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, come definita all'art. 4(12) Regolamento (UE) 2016/679). Inoltre, è necessario proteggere qualsiasi sistema informatico, sistemi di IA inclusi, con misure tecniche e organizzative adeguate al rischio affinché anche l'accesso fisico al medesimo sia reso possibile solo ai soggetti autorizzati (come previsto, ad esempio, dall'art. 32 del GDPR).

3 La sicurezza dei sistemi di Intelligenza Artificiale

Come accennato, i sistemi di IA[26] sono dei sistemi informatici che presentano rischi di cibersicurezza ulteriori rispetto a quelli "tradizionali" in virtù delle loro peculiarità: costituiscono, infatti, dei sistemi complessi, in cui numerose componenti, "intelligenti" e non, interagiscono per tutto il loro ciclo di vita[27].

Oltretutto, l'IA è a "doppio uso": da un lato, è una preziosa risorsa quando viene usata per contrastare le minacce informatiche e rafforzare i relativi strumenti, ad esempio in relazione al rilevamento delle minacce (*threat detection*) e alla risposta agli incidenti (*incident response*) adoperando tecniche di apprendimento automatico (*machine learning*) e *deep learning*[28]; dall'altro lato, costituisce una minaccia quando viene utilizzata per finalità illecite, amplificando notevolmente le capacità offensive degli attaccanti. In altri termini, l'IA può essere utilizzata sia per attaccare sia per difendere.

Tanto precisato, si devono ora prendere in considerazione le più rilevanti minacce informatiche per i sistemi di IA[29], che consistono in:

25. *Ibidem*.

26. Per "sistema di IA", ai sensi dell'art. 3(1) dell'AI Act, deve intendersi "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". Ulteriori specificazioni sulla definizione di sistema di IA sono reperibili nelle relative "Linee guida sulla definizione di un sistema di intelligenza artificiale" della Commissione europea approvate il 6 febbraio 2025 (C(2025) 924 Final). In dottrina si è rilevato, però, che tale nozione "si basa sulla capacità dei sistemi di IA di dedurre da input ricevuti come generare output che influenzano ambienti fisici o virtuali attraverso processi computazionali ad autonomia variabile" e che si espone al rischio "di essere troppo vaga e onnicomprensiva, inglobando sotto l'etichetta di IA una vasta gamma di tecnologie, dai sistemi basati su semplici algoritmi a quelli fondati su apprendimento automatico. La vaghezza definitoria potrebbe portare a problematiche interpretative e applicative, rendendo difficile la distinzione tra ciò che è effettivamente IA e ciò che non lo è", tanto che potrebbe addirittura essere interpretata ricomprendendovi anche software "tradizionali", ove letta unitamente al considerando n. 12 (G. Contissa-F. Galli, *AI Act e diritti fondamentali: presupposti tecnologici e ricadute normative*, in *Quaderni costituzionali*, 2024, 3, pp. 738-739).

27. Come evidenziato dal Gruppo indipendente di esperti ad alto livello sull'intelligenza (istituito dalla Commissione europea nel 2018), affinché si possa ottenere un'IA affidabile è necessario garantire la robustezza tecnica e la resilienza: i sistemi di IA devono essere sviluppati con un approccio di prevenzione dei rischi ed evitando comportamenti inattesi, riducendo al minimo i danni non intenzionali e imprevisti e prevenendo danni inaccettabili, tenendo conto anche dei potenziali cambiamenti nel loro ambiente operativo e di interazioni contraddittorie di altri agenti umani e artificiali. I sistemi di IA devono essere protetti dagli attacchi come gli altri sistemi informatici, tenendo però conto che, rispetto ai secondi, presentano delle specificità dovute alla loro natura: gli attacchi possono colpirne i dati, il modello o l'infrastruttura (hardware e/o software); bisogna inoltre prendere in considerazione le possibili applicazioni non intenzionali di IA (come le applicazioni a duplice uso) e i potenziali abusi di un sistema di IA da parte di soggetti malintenzionati, adottando misure di prevenzione e mitigazione (Gruppo indipendente di esperti ad alto livello sull'intelligenza. Istituito dalla Commissione europea nel giugno 2018, *Orientamenti etici per un'IA affidabile*, Bruxelles, 2019, p. 19).

28. Una tecnica avanzata di *machine learning* utilizzata per apprendere automaticamente da grandi quantità di dati.

29. Per una prospettiva tecnica, cfr., fra gli altri: L. Batina – T. Bäck – I. Buhan – S. Picek (ed.), *Security and Artificial Intelligence. A Crossdisciplinary Approach*, Springer, Cham, 2022; H. Jahankhani – G. Bowen – M.S. Sharif – O. Hussien (ed.), *Cybersecurity and Artificial Intelligence. Transformational Strategies and Disruptive Innovation*, Springer, Cham, 2024; V. Sarveshwaran – J.I-Z. Chen – D. Pelusi (ed.), *Artificial Intelligence and Cyber Security in Industry 4.0*, Springer, Singapore, 2023; M. Stamp – C.A. Visaggio – F. Mercaldo – F. Di Troia (ed.), *Cybersecurity for Artificial Intelligence*, Springer, Cham, 2022.

a) *Data poisoning* (avvelenamento dei dati di addestramento). Si effettua attraverso l'introduzione di informazioni volutamente errate o manipolate nei dataset di training così da alterare le prestazioni e il comportamento del modello di IA, e dunque del sistema, compromettendone accuratezza e affidabilità del sistema (può infatti provocare regressione, errori di classificazione, ecc.); ciò può comportarne l'inutilizzabilità.

b) *Adversarial attacks* (attacchi antagonisti). Sono finalizzati a ingannare il modello mediante input (anche grafici, come le immagini) non percettibili dagli operatori umani, così che il sistema di IA fornisca risposte errate o effettui condotte inattese (minando ad esempio il funzionamento di sistemi di visione artificiale, di riconoscimento vocale o di elaborazione del linguaggio naturale). Di particolare interesse sono gli attacchi antagonisti di tipo *concept drift*: in linea generale, il *concept drift* si ha quando un modello predittivo perde progressivamente accuratezza a causa della modifica dei dati col passare del tempo, rendendo necessario aggiornare il modello o adottare strategie per mantenerne la capacità predittiva. In una prospettiva malevola, invece, si può manipolare in modo graduale (*incremental drift*), improvviso (*sudden drift*) o ricorrente (*recurring drift*) il flusso di dati. In tal modo il sistema non riuscirà a riconoscere le istanze sospette,

c) *Model extraction* (estrazione del modello) e *Model inversion* (inversione del modello). Sono attacchi finalizzati a ricostruire la logica interna del sistema e/o estrarre i dati di addestramento interagendo con il medesimo (ad esempio attraverso le API).

d) *Membership inference* (inferenza sull'appartenenza). Consente di determinare se un dato sia stato incluso nel dataset di addestramento, con potenziale impatto sulla privacy e sulla protezione dei dati personali.

Alla luce di quanto sin qui esposto, può rilevarsi che su ciascun fornitore gravi l'obbligo di garantire la sicurezza a diversi livelli di applicabilità, che spaziano dalla tutela della sicurezza delle persone fisiche alla conservazione dei dati personali, dal mantenimento dell'integrità strutturale del sistema alla protezione e gestione degli asset materiali[30], ma bisogna altresì considerare anche gli utilizzatori dei sistemi di IA devono tenere in debito conto la sicurezza dei sistemi medesimi, essendo comunque responsabili proprio del loro uso, indipendentemente da discipline di settore come l'AI Act.

Pur non essendo questa la sede per una trattazione di quest'ultimo, è bene effettuare una breve notazione in merito ad esso e alla distinzione ivi operata fra i diversi sistemi di IA in base al rischio che i medesimi pongono, con una loro disciplina giuridica differenziata anche per ciò che concerne l'ambito della sicurezza. L'approccio adottato nell'*AI Act* è, infatti, basato sul rischio, ossia, ai sensi del relativo art. 3(3), "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso"; i sistemi di IA vengono classificati in base ai rischi che pongono e le regole sono proporzionate all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. Ciò comporta il divieto di specifiche pratiche di IA considerate inaccettabili, la determinazione di requisiti specifici per i sistemi di IA ad alto rischio e di obblighi per gli operatori pertinenti, nonché di obblighi di trasparenza per i sistemi di IA (considerando n. 26) che pongono rischi limitati; i sistemi a rischio minimo (come i filtri antispam e i videogiochi) sono invece esclusi dall'ambito di applicazione dell'AI Act (fatta salva la possibilità di adesione ai codici di condotta di cui all'art. 95 del Regolamento)[31].

Più ampiamente, nella prospettiva dell'AI Act, come recita il considerando n. 76, "la cibersicurezza svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza".

30. S. Quintarelli – F. Corea – F. Fossa – A. Loreggia – S. Sapienza, *Ai: profili etici. Una prospettiva etica sull'intelligenza artificiale: principi, diritti e raccomandazioni*, in *BioLaw Journal*, 2019, 3, p. 18.

31. Inoltre, nell'AI Act un importante ruolo, anche di garanzia, è giocato proprio dalla sorveglianza umana, come previsto – in particolare – dall'art. 14 per i fornitori e dall'art. 26 per i *deployer*, tanto che l'art. 4 impone a entrambi l'obbligo di adottare misure per garantire, per quanto possibile, un livello sufficiente di alfabetizzazione in materia di IA sia del proprio personale sia di chi opera per proprio conto nell'ambito del funzionamento e dell'utilizzo dei sistemi di IA, il tutto tenendo conto sia delle relative conoscenze tecniche, esperienza, istruzione e formazione, sia del contesto di utilizzo dei sistemi anzidetti sia dei delle persone o dei gruppi su cui detti sistemi devono essere utilizzati.

In tale quadro, il richiamo alla cibersicurezza operato dal legislatore europeo non ha una dimensione meramente tecnica: le vulnerabilità dei sistemi di IA, infatti, non devono essere intese solo come "falle" da colmare mediante soluzioni matematiche, ingegneristiche, informatiche: esprimono, invece, nuove tensioni tra diritti fondamentali, responsabilità e forme di *governance*. È in questa prospettiva che diventa utile elaborare strumenti concettuali e operativi capaci di andare oltre la mera ricognizione descrittiva: basti pensare a matrici normative idonee a correlare specifiche tipologie di attacco con i corrispondenti effetti giuridici e con le possibili misure di prevenzione e controllo, fornendo così una base metodologica per affrontare le trasformazioni tecnologiche in atto con approccio critico e costruttivo.

Riprendendo l'esperienza degli studi di informatica giuridica (con particolare riferimento ad alcune esperienze scandinave, fra cui può qui ricordarsi Jon Bing, in aggiunta al già citato Peter Seipel), è possibile sviluppare strumenti operativi e non meramente ricognitivi, come matrici normative che correlino tipologie di attacco (ad esempio, *data poisoning*, *adversarial attacks, model extraction*) con conseguenze giuridiche (discriminazione algoritmica, violazioni della privacy e dei dati personali, pregiudizi patrimoniali) e con misure di governance idonee (audit terzi, obblighi di documentazione tecnica, clausole contrattuali di sicurezza), come ben evidenziato anche dalle evoluzioni dell'informatica giuridica contemporanea[32].

4 Vulnerabilità delle macchine e delle persone nella Società algoritmica

Quanto sin qui esposto, ancorché succintamente, ha permesso di evidenziare taluni profili di criticità dei sistemi di IA, sia in quanto tali sia in quanto sistemi informatici, e da tale analisi emergono, inequivocabilmente, nuove dimensioni della vulnerabilità sia dei sistemi intelligenti e degli agenti artificiali sia delle persone e dunque degli agenti umani[33].

Difatti, se si guarda all'IA nel suo complesso, appare chiara una vulnerabilità multilivello, che coinvolge dimensioni tecniche, economiche, giuridiche, organizzative e culturali.

Tanto i modelli quanto i sistemi risultano vulnerabili, e tale condizione si riflette sia sugli agenti artificiali e umani sia sugli ambienti – digitali e fisici – in cui essi operano. Ciò dipende dalla pervasiva integrazione dei sistemi di IA nei processi decisionali pubblici e privati, nelle infrastrutture critiche e non, nelle interazioni quotidiane, nella costruzione dell'identità personale e nelle dinamiche relazionali.

Tale quadro impone una riflessione complessiva sulle vulnerabilità non solo degli agenti artificiali e umani, ma anche dei contesti sociali e tecnici in cui essi sono inseriti.

Da un lato, i sistemi di IA presentano vulnerabilità a livello sia strutturale sia funzionale.

Sul piano strutturale, è oramai ben noto che dataset di addestramento spesso opachi o incompleti sono idonei a esporre i modelli a rischi di *data poisoning* e a bias sistematici difficili da individuare e correggere[34].

Sul piano funzionale, le tecniche già menzionate al par. 3 (a titolo esemplificativo, *model inversion*, *membership inference* e *adversarial attacks*) possono alterare le prestazioni o estrarre informazioni sensibili, compromettendo la riservatezza e l'affidabilità degli output. Tali sistemi, inoltre, non sono normalmente "isolati": si

32. Cfr., fra gli altri: G. Corasaniti, *Informatica giuridica e progettazione innovativa digitale*, Wolters Kluwer, Milano, 2024; M. Mancarella (a cura di), *Lineamenti di informatica giuridica*, Tangram, Trento, 2024; G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Giappichelli, Torino, 2022; G. Ziccardi, *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina, Milano, 2022.

33. Del resto, come evidenziato nell'AI Act, l'IA può essere considerata "una famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali" (considerando n. 4). Al contempo, tuttavia, essa può "comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale, compreso il pregiudizio fisico, psicologico, sociale o economico" (considerando n. 5).

34. La problematica dell'opacità e della spiegabilità dell'IA è sempre più attuale e di difficile soluzione nella pratica, in ragione di una complessità sia tecnica sia normativa. Sul punto cfr., fra gli altri: S. Amato, *Inquietudini digitali. Il "black box effect"*, in *Rivista di filosofia del diritto.*, 2025, 1, pp. 33-43; G. Fioriglio, *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici,* cit.; F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge/MA – London, 2015.

registra normalmente, infatti, una interconnessione con reti di fornitori, servizi cloud e componenti software di terze parti; a ciò consegue una moltiplicazione dei punti di attacco (e di potenziali "punti deboli"), rendendo comunque più complessa la gestione unitaria della sicurezza. Inoltre, in ragione dell'opacità e della complessità tecnica e contrattuale fra una molteplicità di attori diversi, magari collocati in aree geografiche lontane (e sottoposte a diverse giurisdizioni), diviene arduo giungere ad attribuire correttamente le responsabilità e imporre standard uniformi di protezione.

Dall'altro, gli esseri umani sono per loro natura vulnerabili, ma alcuni lo sono più di altri, permanentemente o temporaneamente (come nel caso di una patologia o della minore età)[35]: l'interazione costante nella società algoritmica può renderli ancora più fragili in conseguenza di azioni di agenti artificiali, umani o loro combinazioni, tenendo conto della necessaria distinzione fra persone di minore e di maggiore età per ciò che concerne l'adozione effettiva ed efficace di strumenti di *cybersecurity by design*. Com'è noto, infatti, fra le persone maggiormente vulnerabili rientrano proprio i minori: essi sono, in linea generale, esposti "a una serie di minacce che spazia dai crimini tradizionali a nuove forme di persecuzione e aggressione, come adescamento online, truffe ed estorsioni, cyberbullismo", con ulteriori rischi in caso di utilizzo di tecnologie avanzate e di compromissione di dispositivi cyber-fisici che "consente all'attaccante di manipolare l'esperienza immersiva, estendendo potenzialmente l'intrusione anche alla sfera emotiva e corporea dell'utente"[36]. Nella predisposizione e nella regolamentazione delle misure di protezione e di garanzia della cibersicurezza, l'IA si presenta come un'arma a doppio taglio. Può infatti contribuire ad accrescere la vulnerabilità dei minori, oppure, al contrario, offrire strumenti di tutela più efficaci. Numerose sono le soluzioni tecniche ad oggi disponibili, che spaziano dalle varie forme di controllo parentale a sistemi di verifica dell'età per accedere a siti web, ma la strada verso una protezione effettiva dei minori è ancora lunga anche per ciò che concerne i profili di cibersicurezza. Anche in questo caso, non è sufficiente limitarsi ai profili meramente tecnici e operativi (come la sola descrizione tecnica degli strumenti disponibili): occorre interrogarsi sul ruolo che il diritto deve assumere di fronte a tali vulnerabilità. Ci troviamo, però, su un piano scivoloso, stretti fra censura dei contenuti e diritto alla libera manifestazione del pensiero, fra società globale e ordinamenti nazionali, fra libero mercato e ampia disponibilità di prodotti e servizi insicuri e privi di qualsiasi garanzia di sicurezza (dalle telecamere di sorveglianza per uso domestico ai dispositivi indossabili).

Se il diritto fatica a trovare delle soluzioni realmente condivise, la risposta può giungere – in particolare – da una corretta formazione non solo all'uso delle tecnologie (componente informatica) ma anche alle conseguenze giuridiche dell'utilizzo medesimo, lecito o illecito che sia (componente giuridica).

Ciò vale anche per le persone maggiorenni. Basti pensare, nel ciberspazio, alla predisposizione a subire attacchi di *social engineering*, all'effettuazione di una determinata condotta quale conseguenza di algoritmi di raccomandazione e filtraggio, all'asimmetria informativa e contrattuale verso le Big Tech.

Per completare il quadro ai fini del presente contributo, non essendo questa la sede per una mappatura completa di tutte le problematiche che sorgono, bisogna altresì tener conto della crescente dipendenza cognitiva da strumenti automatizzati di supporto alla decisione che, in ipotesi, possono sostituirsi proprio all'agente umano, che viene profilato e sorvegliato dai predetti algoritmi, le cui elaborazioni possono poi guidare l'azione di altri agenti intelligenti nell'orientare le decisioni e gli atti della persona medesima.

Vi è di più.

Tanto le "macchine" quanto le persone operano nel ciberspazio, caratterizzato non solo da flussi informativi incessanti e in continua espansione, ma anche dall'idoneità a produrre effetti al di fuori del ciberspazio medes-

35. Sulla vulnerabilità cfr. T. Casadei, *La vulnerabilità in prospettiva critica*, in O. Giolo – B. Pastore (a cura di), *Vulnerabilità. Analisi critica di un soggetto*, Carocci, Roma, pp. 73-99; A. Di Giandomenico – C. Diodati – F. Ricci, *vulnerabilità come risorsa e come valorizzazione della differenza nelle democrazie contemporanee. Profili giuridici, sociologici ed etico-politici*, Mimesis, Milano, 2021; F. Macioce, *La vulnerabilità di gruppo: funzione e limiti di un concetto controverso*, Giappichelli, Torino, 2021; B. Pastore, *semantica della vulnerabilità, soggetto, cultura giuridica*, Giappichelli, Torino, 2021; S. Dadà, *Vulnerabilità digitale. Etica, Intelligenza Artificiale e Medicina*, Mimesis, Milano, 2024; G. Zanetti, *Filosofia della vulnerabilità. Discriminazione, percezione, diritto*, Carocci, Roma, 2019.

36. R. Brighi – V. Ferrari, *(Cyber)sicurezza e infanzia digitale. Oltre la protezione, verso un uso critico e consapevole della tecnologia*, in T. Casadei – V. Barone – B. Rossi (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025, pp. 25-26.

imo: ciò nonostante, la regolamentazione "istituzionale" risulta sovente meno rilevante ed efficace rispetto ai contratti e alle policy delle Big Tech. Proprio quest'ultimi sono redatti unilateralmente e a favore delle Big Tech medesime, oltre che imposti agli utenti come *condicio sine qua non* per l'accesso a servizi e ambienti virtuali, con conseguente esclusione di chi non li accetta. Si tratta, a ben vedere, di veri e propri "scambi senza accordo"[37], nei quali lo squilibrio che si realizza "può tradursi in vere e proprie forme di dominio"[38]).

In tale contesto, le decisioni e le condotte di agenti artificiali[39] e umani risultano vulnerabili a forme più o meno esplicite di condizionamento: i primi possono essere manipolati attraverso interventi sugli input o sulla configurazione dei modelli, al fine di orientarne gli output; i secondi possono subire influenze mediante meccanismi di *nudging*[40], strategie di profilazione[41] predittiva e altre tecniche persuasive integrate nelle architetture decisionali.

Inoltre, l'enorme, crescente e sostanzialmente incontrollato flusso di informazioni (raccolte, elaborate, create) contribuisce a plasmare la società sia partecipando al funzionamento di diversi settori (creditizio, commercio, sanitario, ecc.) sia introducendo o perpetuando discriminazioni sia consentendo una sempre più sofisticata sorveglianza di massa[42], e portando potenzialmente anche a una "disinformazione aumentata" (ossia "l'insieme delle trasformazioni che il fenomeno della disinformazione subisce in conseguenza dell'integrazione dell'IA nei processi di produzione, diffusione e gestione dei contenuti informativi. L'IA agisce come un potente moltiplicatore, capace sia di rendere la disinformazione più veloce, personalizzata e convincente, sia di offrire strumenti efficaci per contrastarla. In questo senso, essa rappresenta un vero e proprio"Giano bifronte" del sistema (dis-)informativo contemporaneo: da un lato abilita nuove minacce, dall'altro sostiene la difesa dell'informazione veritiera"[43]).

Pertanto, alle "tradizionali" vulnerabilità se ne aggiungono altre, e tutte costituiscono elementi strutturali dell'odierno ecosistema digitale. Non v'è dubbio che la risposta degli ordinamenti giuridici non possa oramai essere né tardiva né meramente reattiva: deve pertanto adottarsi un nuovo modello proattivo, ancorato ai principi di *security by design* e di *accountability*, garantendo necessariamente una possibilità concreta di *audit*, previe adozione di standard tecnici interoperabili, certificazione periodica dei sistemi e imposizione di obblighi informativi che siano realmente chiari e comprensibili, con predisposizione di strumenti di tutela effettiva per cercare di bilanciare rapporti contrattuali fortemente squilibrati.

Non vi è dubbio che le criticità siano molteplici e intersechino aspetti tecnici, etici e giuridici che investono la stessa struttura degli ordinamenti democratici, e che spingono anche a "chiederci a quale scopo dovremmo sviluppare certe tecnologie, e non altre", scindendo la capacità tecnica (il *saper* fare) dall'opportunità normativa (il *dover* fare)"[44].

Torna, ancora una volta, la necessità, più che l'opportunità, di adottare la già menzionata prospettiva informatico-giuridica per evitare che all'evoluzione meramente tecnologica dell'IA (e di tutti quei servizi e artefatti che l'adoperano in modo più o meno marcato) consegua un'involuzione degli ordinamenti giuridici,

37. Cfr. N. Irti, *Scambi senza accordo*, in *Rivista trimestrale di diritto civile*, 1998, 2, pp. 347-364.

38. M.N. Campagnoli – M. Farina, *Identità digitale e intelligenza artificiale: tra regolazione, poteri asimmetrici e sfide per il futuro*, in *JELT – Journal of Ethics and Legal Technologies*, 2025, 7(1), p. 100.

39. Sui profili informatico-giuridici delle decisioni algoritmiche cfr.: G. D'Acquisto, *Decisioni algoritmiche. Equità, causalità, trasparenza*, Giappichelli, 2022; A. Santosuosso – G. Sartor, *Decidere con l'IA. Intelligenze artificiali e naturali nel diritto*, Il Mulino, Bologna, 2024; S. Sapienza, *Decisioni algoritmiche e diritto*, Giuffrè Francis Lefebvre, Milano, 2024.

40. Sul *nudging* cfr., in particolare, R.H. Thaler – C.R. Sunstein, *Nudge. The Final Edition*, Penguin Books, London, 2021.

41. Cfr., fra gli altri, F. Lagioia – G. Sartor, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 2020, 11, pp. 85-110.

42. Cfr. S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, tr. it., Luiss University Press, II ed., Roma, 2023.

43. G. Contissa – F. Galli, *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, in *Federalismi.it*, 2025, 15, p. 131.

44. S. Vantin, *Dalla cibernetica all'intelligenza artificiale. Ascesa e declino del dibattito sullo scopo*, in *Ordines*, 2024, 2, p. 305.

sacrificando i diritti alla tecnologia e al mercato[45]. Un ruolo anticipatorio e proattivo del diritto, dunque, che – mutuando una terminologia informatica – renda le tecnologie realmente "interoperabili" con gli ordinamenti giuridici, consentendone la valutazione tanto *ex ante* quanto *ex post*. Nello scenario qui tratteggiato assumono particolare rilevanza i profili di cibersicurezza e, in particolare, gli attacchi mirati ai sistemi di IA: alterandone l'accuratezza, possono produrre effetti a catena sull'operato di coloro che su di essi fanno affidamento.

Il compito del legislatore è, dunque, particolarmente complesso.

È indispensabile un approccio interdisciplinare – e non semplicemente multidisciplinare – in cui informatica, etica, statistica, diritto e altre competenze interagiscano e si contaminino reciprocamente, condividendo concetti, metodologie e finalità.

Solo così sarà possibile definire un quadro regolatorio capace di orientare lo sviluppo dell'intelligenza artificiale senza soffocarne il potenziale innovativo, assicurando che essa non operi "in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana" (art. 41 Cost.), senza tuttavia dimenticare che le tecnologie sono pur sempre "espressione del nostro essere animali parlanti. Forse la sfida cui il nostro tempo ci chiama non è a ripensare il rapporto tra la nostra natura e la tecnica, bensì a prendere sul serio la lezione di certa antropologia filosofica e riscoprire la nostra natura tecnica"[46].

Bibliografia

S. Amato, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020.

S. Amato, *Inquietudini digitali. Il "black box effect"*, in *Rivista di filosofia del diritto.*, 2025, 1, pp. 33-43.

S. Aterno, *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, Pisa, 2022.

J. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal*, Vol. 78, 5, 2017, pp. 1217-1241.

W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithmics*, Cambridge University Press, Cambridge, 2020.

L. Batina-T. Bäck-I. Buhan-S. Picek (ed.), *Security and Artificial Intelligence. A Crossdisciplinary Approach*, Springer, Cham, 2022.

R. Brighi, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in T. Casadei-S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Seconda edizione aggiornata e ampliata. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali,* Wolters Kluwer, Milano, 2024, pp. 75-87.

R. Brighi, *Cybersicurezza e intelligenza artificiale. Un'analisi critica*, in *BioLaw Journal*, 2024, 1 (special issue), pp. 111-124.

45. Un esempio di "sacrificio" di un diritto può essere rinvenuto nel diritto alla protezione dei dati personali: proprio i dati costituiscono infatti una "merce di scambio" adoperata sovente per usufruire di determinati servizi, verificandosi così la loro monetizzazione (cfr., in particolare, G. Cerrina Feroni (a cura di), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Il Mulino, Bologna, 2024). Basti pensare, in tal senso, ai "cookie wall" e alla possibilità di scegliere se pagare un determinato corrispettivo oppure lasciarsi profilare per poter consultare un determinato sito web. Ma, in linea più generale, è necessario interrogarsi non solo sui profili giuridici, ma anche su quelli etici: inoltre, come evidenziato da Antonio Punzi, l'accelerazione del tempo non concede quel tempo che un consenso consapevole richiederebbe – per cui potrebbe ipotizzarsi il recupero della dimensione dialogica nella formazione del consenso medesimo grazie all'interazione con le IA che potrebbero in futuro eseguire le volontà di ciascun interessato (in tal senso A. Punzi, *È eticamente accettabile – e se sì a quali condizioni – fare commercio dei propri dati*?, in G. Cerrina Feroni (a cura di), *Commerciabilità dei dati personali*, cit., pp. 69-86).

46. A. Punzi, *Scambi (digitali) senza accordo? Logos, tecnocapitalismo ed ermeneutica della contemporaneità*, in G. Vettori (a cura di), *Giuseppe Benedetti e il Governo del Forse*, Cedam - Wolters Kluwer, Milano, 2023, p. 182.

R. Brighi-V. Ferrari, *(Cyber)sicurezza e infanzia digitale. Oltre la protezione, verso un uso critico e consapevole della tecnologia*, in T. Casadei – V. Barone – B. Rossi (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025, pp. 15-30.

M.N. Campagnoli – M. Farina, *Identità digitale e intelligenza artificiale: tra regolazione, poteri asimmetrici e sfide per il futuro*, in *JELT – Journal of Ethics and Legal Technologies*, 2025, 7(1), pp. 81-115.

T. Casadei, *La vulnerabilità in prospettiva critica*, in O. Giolo – B. Pastore (a cura di), *Vulnerabilità. Analisi critica di un soggetto*, Carocci, Roma, pp. 73-99.

T. Casadei – V. Barone – B. Rossi (a cura di), *Giovani in rete. Guida per un uso consapevole delle tecnologie*, Giappichelli, Torino, 2025.

T. Casadei-S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Seconda edizione aggiornata e ampliata. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali,* Wolters Kluwer.

T. Casadei-S. Pietropaoli, *Intelligenza artificiale: l'ultima sfida per il diritto?*, in Id. (a cura di), *Diritto e tecnologie informatiche. Seconda edizione aggiornata e ampliata. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 259-274;

F. Casarosa-G. Comandé, *Aspettando la NIS2: ovvero il diritto privato della Cybersecurity*, in *Il Diritto dell'informazione e dell'Informatica*, 2024, 1, pp. 29-53.

G. Cerrina Feroni (a cura di), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Il Mulino, Bologna, 2024.

P.G. Chiara-R. Brighi, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 21, 2021, pp. 18-42.

G. Contissa, *Information Techonology for the Law*, Giappichelli, Torino, 2017.

G. Contissa-F. Galli, *AI Act e diritti fondamentali: presupposti tecnologici e ricadute normative*, in *Quaderni costituzionali*, 2024, 3, pp. 738-741.

G. Contissa – F. Galli, *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, in *Federalismi.it*, 2025, 15, pp. 126-156.

G. Corasaniti, *Informatica giuridica e progettazione innovativa digitale*, Wolters Kluwer, Milano, 2024.

L. Corso, *Legge dell'algoritmo e rule of law. Riflessioni preliminari*, in *PasSaggi costituzionali*, 2024, 1, pp. 201-214.

S. Dadà, *Vulnerabilità digitale. Etica, Intelligenza Artificiale e Medicina*, Mimesis, Milano, 2024.

G. D'Acquisto, *Decisioni algoritmiche. Equità, causalità, trasparenza*, Giappichelli, Torino, 2022.

G. De Gregorio-P. Dunn, *The European risk-based approaches: connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, 59, pp. 476-477.

A. Di Giandomenico – C. Diodati – F. Ricci, *vulnerabilità come risorsa e come valorizzazione della differenza nelle democrazie contemporanee. Profili giuridici, sociologici ed etico-politici*, Mimesis, Milano, 2021.

L.A. Dimatteo – C. Poncibò – M. Cannarsa (edited by), *The Cambridge handbook of artificial intelligence. Global perspectives on law and ethics*, Cambridge University Press, Cambridge, 2022.

F. Donati – G. Finocchiaro – F. Paolucci – O. Pollicino (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè Francis Lefebvre, Milano, 2025.

ENISA, *ENISA overview of cybersecurity and related terminology*, Heraklion, 2017.

ENISA, *ENISA threat landscape 2024*, Attiki-Heraklion-Brussels, 2024.

G. Finocchiaro, *Diritto dell'intelligenza artificiale*, Zanichelli, Bologna, 2024.

G. Fioriglio, *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici,* in *Ars interpretandi*, 2021, 1, pp. 53-67.

G. Fioriglio, *Temi di informatica giuridica*, Aracne, Roma, 2004.

V. Frosini, *Cibernetica, diritto e società*, Roma Tre Press, Roma, (1968) 2023.

L. Floridi, *Etica dell'intelligenza artificiale, sviluppi, opportunità, sfide*, Raffaele Cortina, Milano, 2022.

T.F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni Costituzionali*, 2024, 2, pp. 277-304.

G. Gorgoni, *Stay Human. The quest for Responsability in the Algorithmic Sociey*, in *Journal of Ethics and Legal Technologies*, 2, 2020, pp. 31-47.

B. Indovina, *Informatica, diritto, intelligenza artificiale*, EGEA, Milano, 2024.

N. Irti, *Scambi senza accordo*, in *Rivista trimestrale di diritto civile*, 1998, 2, pp. 347-364.

H. Jahankhani-G. Bowen-M.S. Sharif-O. Hussien (ed.), *Cybersecurity and Artificial Intelligence. Transformational Strategies and Disruptive Innovation*, Springer, Cham, 2024.

F. Lagioia – G. Sartor, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 2020, 11, pp. 85-110.

F.H. Llano Alonso, *Homo ex machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnòlogica*, Tirant lo Blanch, Valencia, 2024.

E. Longo, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna parlamentare*, 2024, 2, pp. 313-347.

M.G. Losano, *Scritti di informatica e diritto. Per una storia dell'informatica giuridica* (a cura di P. Garbarino-M. Cavino), Mimesis, Milano, 2022.

F. Macioce, *La vulnerabilità di gruppo: funzione e limiti di un concetto controverso*, Giappichelli, Torino, 2021.

M. Mancarella (a cura di), *Lineamenti di informatica giuridica*, Tangram, Trento, 2024.

H.W. Micklitz-O. Pollicino-A. Simoncini-G. Sartor-G. De Gregorio (ed.), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021.

F.P. Micozzi, *Sicurezza informatica. Obblighi e responsabilità dopo il recepimento della NIS2 e la l. n. 90/2024*, Wolters Kluwer, Milano, 2024.

L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, 14, 2024, pp. 179-197.

L. Palazzani, *Etica della regolazione dell'intelligenza artificiale*, in *Rivista di filosofia del diritto.*, 2025, 1, pp. 9-2.

L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Studium, Roma, 2020.

F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge/MA – London, 2015.

F. Pasquale, *Towards a Fourth Law of Robotics: Preserving Attribution, Responsability and Explanaibility in an Algorithmic Society*, in *Ohio State Law Journal*, 2017, 78, pp. 1243-1255.

B. Pastore, *semantica della vulnerabilità, soggetto, cultura giuridica*, Giappichelli, Torino, 2021.

G. Peruginelli-M. Ragona (a cura di), *L'informatica giuridica in Italia*, Edizioni Scientifiche Italiane, Napoli, 2014.

M. Pietrangelo, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista italiana di informatica e diritto*, 2024, 2, pp. 14-24.

S. Pietropaoli, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Giappichelli, Torino, II ed., 2025.

M.G. Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technlogy Analysis*, Bloomsbury, London, 2023.

A. Punzi, *È eticamente accettabile – e se sì a quali condizioni – fare commercio dei propri dati*?, in G. Cerrina Feroni (a cura di), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Il Mulino, Bologna, 2024, pp. 69-86.

A. Punzi, *Scambi (digitali) senza accordo? Logos, tecnocapitalismo ed ermeneutica della contemporaneità*, in G. Vettori (a cura di), *Giuseppe Benedetti e il Governo del Forse*, Cedam - Wolters Kluwer, Milano, 2023, pp. 173-187.

S. Quintarelli-F. Corea-F. Fossa-A. Loreggia-S. Sapienza, *Ai: profili etici. Una prospettiva etica sull'intelligenza artificiale: principi, diritti e raccomandazioni*, in *BioLaw Journal*, 2019, 3, pp. 159-177.

F. Romeo, *Il diritto artificiale*, Giappichelli, Torino, 2002.

P. Moro-C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, FrancoAngeli, Milano, 2017.

S. Russell-P. Norvig, *Artificial Intelligence: A Modern Approach*, *Global Edition*, Pearson, Harlow, 4th edition, 2022.

S. Salardi, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, Giappichelli, Torino, 2022.

A. Santosuosso – G. Sartor, *Decidere con l'IA. Intelligenze artificiali e naturali nel diritto*, Il Mulino, Bologna, 2024.

S. Sapienza, *Decisioni algoritmiche e diritto*, Giuffrè Francis Lefebvre, Milano, 2024.

G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Giappichelli, Torino, 2022.

G. Sartor, *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022.

V. Sarveshwaran-J.I-Z. Chen-D. Pelusi (ed.), *Artificial Intelligence and Cyber Security in Industry 4.0*, Springer, Singapore, 2023.

A. Segura-Serrano (ed.), *Global Cybersecurity and International Law*, Taylor-Francis, New York and London, 2024.

P. Seipel, *ICT Law – A Kaleidoscope View*, in *Scandinavian Studies in Law – ICT Legal Issues*, 2010, pp. 33-58.

M. Schuilenburg-R. Peeters (ed.), *The Algorithmic Society. Technology, Power and Knowledge*, Routledge, London, 2021.

E. Sorrentino-A.F. Spagnuolo, *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in *Rivista italiana di informatica e diritto*, 2024, 2, pp. 685-701.

M. Stamp-C.A. Visaggio-F. Mercaldo-F. Di Troia (ed.), *Cybersecurity for Artificial Intelligence*, Springer, Cham, 2022.

R.H. Thaler – C.R. Sunstein, *Nudge. The Final Edition*, Penguin Books, London, 2021.

R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Franco Angeli, Milano, 2023.

S. Vantin, *Dalla cibernetica all'intelligenza artificiale. Ascesa e declino del dibattito sullo scopo*, in *Ordines*, 2024, 2, pp. 285-306.

A. Venanzoni, *L'ordine costituzionale della cybersecurity, in Forum di Quaderni Costituzionali*, 2024, 4, pp. 33-80.

G. Vettori (a cura di), *Giuseppe Benedetti e il Governo del Forse*, Cedam - Wolters Kluwer, Milano, 2023.

G. Zanetti, *Filosofia della vulnerabilità. Discriminazione, percezione, diritto*, Carocci, Roma, 2019.

G. Ziccardi, *Dati avvelenati. Truffe, virus informatici e falso online*, Raffaello Cortina, Milano, 2024.

G. Ziccardi, *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina, Milano, 2022.

S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, tr. it., Luiss University Press, II ed., Roma, 2023.