*Ciberspazio e diritto*, vol. 26, n. 79 (1 - 2025), pp. 195-218

# Danni sistemici, risarcimento collettivo: il caso della discriminazione algoritmica attraverso la pubblicità mirata

Malwina Anna Wójcik-Suffia*

Sommario: 1. Introduzione. – 2. *Beaulieu c. Facebook.* – 2.1. Fatti e procedura. – 2.2. La sentenza della Corte d'appello del Québec. – 2.2.1 – La presenza di questioni comuni. – 2.2.2 – Composizione del gruppo. – 3. *Global Witness Foundation e Clara Wichmann Bureau Foundation c. Meta*. – 3.1. Fatti e procedura. – 3.2. La decisione dell'Istituto olandese per i diritti umani. – 3.2.1. Competenza e ammissibilità. – 3.2.2. L'applicabilità della legge olandese contro la discriminazione. – 3.2.3. La presenza di discriminazione. – 4. Verso un approccio sistemico alla discriminazione attraverso la pubblicità mirata. – 5. Il futuro della regolamentazione dell'UE in materia di pregiudizi nella pubblicità mirata: nuove opportunità procedurali per il risarcimento collettivo. – 6. Conclusione.

## 1. *Introduzione*

Le carenze della legislazione antidiscriminatoria nell'affrontare la discriminazione algoritmica sono state ampiamente discusse dagli studiosi[1]. Oltre alla portata personale e materiale limitata, i ricorrenti hanno difficoltà a individuare pratiche potenzialmente discriminatorie e a produrre prove per stabilire un caso di discriminazione *prima facie*. Questi

* L'Autrice ha conseguito un dottorato di ricerca internazionale presso le Università di Bologna e del Lussemburgo, sul tema delle discriminazioni algoritmiche in ambito sanitario. È assegnista di ricerca presso l'Università degli Studi di Milano.

[1] Cfr. ad esempio: H. Weerts, et al., *Algorithmic Unfairness through the Lens of EU Non-Discrimination Law: Or Why the Law Is Not a Decision Tree*, Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, FAccT '23 805, 2023; S. Wachter, B. Mittelstadt, C. Russell, "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI", «Computer Law & Security Review», 2021, 41.

problemi sorgono spesso nel contesto della pubblicità mirata su grandi piattaforme online, una pratica che consente agli inserzionisti di specificare i criteri o gli attributi che un consumatore a cui viene mostrato l'annuncio dovrebbe avere. Piattaforme come Facebook o LinkedIn raccolgono una grande quantità di dati personali sugli utenti, tra cui caratteristiche demografiche, comportamentali e di interesse, che gli inserzionisti possono sfruttare per il targeting[2]. Sulla base dei parametri scelti dall'inserzionista, le piattaforme pubblicitarie utilizzano algoritmi di ottimizzazione per decidere il pubblico più adatto all'annuncio[3]. La pratica della pubblicità mirata può perpetuare modelli discriminatori nell'accesso a opportunità cruciali, tra cui l'occupazione e l'alloggio, anche in assenza di istruzioni dirette da parte dell'inserzionista di escludere un particolare gruppo protetto. Ad esempio, quando il comportamento degli utenti nel tempo esprime risposte stereotipate a determinati annunci di lavoro, l'algoritmo potrebbe incorporare tali modelli storici, limitando potenzialmente l'accesso alle opportunità per determinati gruppi.[4] Tale negazione di opportunità causa un danno diretto a individui specifici, che spesso rimangono inconsapevoli della discriminazione subita. Inoltre, dal punto di vista sistemico, la pubblicità mirata porta a danni sociali, tra cui il rafforzamento degli stereotipi di genere, età o razza e gli squilibri di potere.

Negli ultimi due anni, le accuse di discriminazione attraverso la pubblicità mirata da parte delle piattaforme di social media sono aumentate vertiginosamente in varie giurisdizioni in tutto il mondo. Questo articolo analizza attentamente due casi recenti che hanno preso in esame la discriminazione perpetuata dagli algoritmi di targeting pubblicitario di Facebook. Il primo caso, *Beaulieu c. Facebook,* è una sentenza[5] della Corte d'appello del Quebec che autorizza un'azione collettiva contro Facebo-

[2] Cfr. T. Speicher, et al., *Potential for Discrimination in Online Targeted Advertising*, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:5-19, 2018.

[3] Cfr. B. Imana, A. Korolova, J. Heidemann, *Auditing for Discrimination in Algorithms Delivering Job Ads*, Proceedings of the Web Conference 2021 (WWW '21), Ljubljana, Slovenia. ACM, New York, NY, 2021. https://doi. org/10.1145/3442381.3450077.

[4] Cfr. T. Speicher, et al., *Potential for Discrimination in Online Targeted Advertising*, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:5-19, 2018.

[5] Cfr. *Beaulieu c. Facebook inc.* 2022 QCCA 1736.

*Danni sistemici, risarcimento collettivo: il caso della discriminazione algoritmica attraverso la pubblicità mirata*

Questo articolo sostiene che le pratiche di pubblicità mirata basate sull'intelligenza artificiale, che consolidano l'esclusione strutturale dei gruppi vulnerabili dalle opportunità, giustificano meccanismi di risarcimento collettivo. Si basa su due casi recenti riguardanti l'algoritmo di targeting pubblicitario di Meta. Nel *caso Beaulieu v. Facebook,* la Corte d'appello del Quebec ha autorizzato un'azione collettiva, interpretando in modo estensivo le questioni comuni e l'appartenenza al gruppo, per riflettere la natura sistemica e l'opacità degli algoritmi di distribuzione degli annunci pubblicitari. Nel caso *Global Witness & Clara Wichmann c. Meta,* una causa di interesse pubblico intentata da organizzazioni non governative, lo Netherlands Institute of Human Rights ha deciso che il sistema pubblicitario di Meta costituiva una discriminazione indiretta di genere nella fornitura di servizi. Insieme, queste decisioni illustrano come le procedure rappresentative o di interesse pubblico possano affrontare danni diffusi e spesso invisibili. Sulla base degli insegnamenti tratti dai casi, l'articolo propone che il rafforzamento degli organismi per la parità e l'estensione del ricorso collettivo nell'UE potrebbero essere una via da seguire per affrontare la distorsione algoritmica su larga scala.

*Systemic Harms, Collective Redress: The Case of Algorithmic Discrimination by Targeted Advertising*

This article argues that AI-based targeted advertising practices that entrench structural exclusion of vulnerable groups from opportunities, warrant collective redress mechanisms. It draws on two recent cases concerning the ad targeting algorithm of Meta. In *Beaulieu v. Facebook*, the Quebec Court of Appeal authorised a class action, reading common issues and group membership expansively to reflect the systemic nature and opacity of ad-delivery algorithms. In *Global Witness & Clara Wichmann v. Meta*, a public interest case brought by non-governmental organisations, the Netherlands Institute of Human Rights decided that Meta's ad system amounted to indirect gender discrimination in the provision of services. Together, these decisions illustrate how representative or public-interest procedures can address diffuse, often invisible harms. Building on lessons from the cases, the article proposes that empowering equality bodies and extending collective redress in the EU could be a way forward to tackle algorithmic bias at scale.

*Ciberspazio e diritto*, vol. 26, n. 80 (2 - 2025), pp. 219-259

# Autodeterminazione contrattuale, intelligenza artificiale e diritti umani: la costruzione della volontà dematerializzata

Federico Zumpani*

Sommario: 1. Introduzione: l'impatto delle nuove tecnologie nella sistematica civilistica. – 2. L'accoglimento degli smart contract nei traffici giuridici e i profili di criticità applicative. – 3. Gli effetti degli smart contract sui diritti umani: rilievi patologici della tecnologia blockchain. – 4. L'interazione fra diritto internazionale privato e diritti umani negli smart contract: la giurisdizione decentralizzata e il conflitto di leggi nella dimensione telematica. – 5. Il rapporto tra *lex cryptographia* e diritto internazionale dei diritti umani: profili di ingegneria giuridica. – 6. Conclusioni: il riconoscimento dei *digital rights* come limite agli smart contract.

## 1. *Introduzione: l'impatto delle nuove tecnologie nella sistematica civilistica*

L'implementazione dei sistemi informatici, telematici e cibernetici nella prassi commerciale e nei traffici giuridici ha gradualmente contribuito a mutare l'impianto dogmatico tradizionale della volontà individuale.

La necessità di un progresso tecnologico giustificato dall'esigenza di semplificare, modernizzare e rinnovare la realtà giuridico-economica è il preludio di un rinnovamento delle interrelazioni giuridiche, da cui deriva l'obbligo generale di garantire un presidio rafforzato di diritti e libertà attinenti alla sfera dell'autonomia privata[1].

* Nato a Palermo nel 1984, laurea magistrale in giurisprudenza, ha svolto fino al 2023 l'attività di avvocato, occupandosi principalmente di diritto civile. Ha conseguito il titolo di Ph.D. in diritti umani presso l'Università di Palermo nel 2015, dopo aver svolto anche un periodo di ricerca a Londra, e ha partecipato, come relatore, a convegni e seminari presso l'Università di Cambridge. Ha, inoltre, ricoperto incarichi di insegnamento di diritto costituzionale, diritto dell'Unione europea e diritto internazionale presso enti

La legittimazione di una regola tecnica sovrapposta alla norma giuridica necessita di costruzioni argomentative e giustificative equilibrate che assicurino ai consociati forme di garanzia adeguate in termini di tutela dei diritti fondamentali[2].

Indubbiamente, i principali effetti derivanti da tale evoluzione digitale si ripercuotono sulla sfera individuale, configurando potenziali pregiudizi alla sfera dei diritti della persona, destinati ad un adeguamento strutturale al suddetto progresso[3].

Preliminarmente, il riconoscimento di una dignità giuridica all'automazione sottende l'analisi dell'impianto dogmatico dell'algoritmo come presupposto della volontà contrattuale, senza mai dimenticare l'originario assetto antropocentrico dell'autodeterminazione privata. Infatti, la digitalizzazione delle relazioni economiche condiziona il ruolo dell'attività umana nell'interrelazione giuridica, configurandosi ancora soggettività ibride in cui la dimensione artificiale del macchinario considera l'attività umana come parte integrante. La compenetrazione tra entità digitale e *agere* umano può essere concettualizzata come nucleo di una più generale tendenza ad ibridare spazi e sfere d'azione differenti[4].

universitari e, attualmente, svolge l'attività di assistente giuridico e amministrativo presso il T.A.R. Palermo.

[1] In riferimento al criterio della volontà, occorre evidenziare, nella dimensione giuridica, la rilevanza attribuita al c.d. meccanismo dell'apprendimento automatico (*machine learning*), ossia lo strumento che consente ai sistemi di intelligenza artificiale di evolvere, apprendere e prendere decisioni in modo autonomo, in funzione della loro esperienza, con scelte talvolta non prevedibili. In proposito, cfr. G. Sartor, A. Omicini, *The autonomy of technological systems and responsibilities for their use*, in *Autonomous Weapon Systems. Law, Ethics, Policy*, Cambridge, 2016, pp. 39 e ss.

[2] Cfr. L. Marini, *Il commercio elettronico. Profili del diritto comunitario*, Padova, Cedam, 2000.

[3] Cfr. A. Santosuosso, *Diritto, scienza, nuove tecnologie*, Padova, Cedam, 2011.

[4] Cfr. E. Armano, S. Cominu, *Connettività e capacità umana nella trasformazione digitale*, in C. Benvegnù, N. Cuppini, M. Frapporti, F. Milesi, M. Pirone, (a cura di), *Capitalismo 4.0. Genealogia della rivoluzione digitale*, Milano, Meltemi, 2021, p. 126. Secondo gli Autori, la connettività struttura in modo ambivalente la società digitale, nel senso che essa, da un lato, non solo si presenta come potenza liberatoria che enfatizza la dimensione di immediatezza, velocità e flusso, ma mostra la "conoscenza" sempre più accessibile e fornisce ulteriori gradi di autonomia ai soggetti con la possibilità di costruire relazioni al di là dei vincoli di tempo e spazio. Invece, dall'altro lato, la possibilità di "esserci sempre" (o l'ingiunzione alla reperibilità permanente) comporta l'indistinzione tra vita e lavoro.

*Autodeterminazione contrattuale, intelligenza artificiale e diritti umani: la costruzione della volontà dematerializzata*

L'evoluzione della realtà tecnologica, attraverso l'implementazione di meccanismi crittografici e algoritmi, ha invaso inevitabilmente la dimensione contrattuale, influenzando non solo la volontà negoziale, ma anche il ruolo concreto delle parti nel perseguimento degli interessi reciproci. Inoltre, gli effetti dell'automazione sulla programmazione contrattuale sottendono una pluralità di profili patologici sotto il profilo della distinzione fra *agere* umano e soggettività virtuale. Il contributo si pone l'obiettivo, in primo luogo, di individuare la progressiva dematerializzazione della volontà negoziale determinata dall'avvento delle c.d. nuove tecnologie, analizzando le principali categorie specifiche in cui è configurabile la struttura informatica di un rapporto contrattuale e con particolare riferimento ai c.d. smart contract, un nuovo istituto giuridico foriero di un ecosistema giuridico virtuale. Indubbiamente, l'analisi di questa nuova fattispecie negoziale determina la nascita di nuove situazioni giuridiche soggettive da tutelare, in quanto l'esecuzione automatizzata di un contratto "intelligente" può determinare un travalicamento del ruolo delle parti, tale da causare una potenziale violazione sistematica dei diritti umani. Infatti, gli effetti della c.d. tecnologia blockchain nell'ambito dei vincoli fra i contraenti, implicano l'attuazione di un meccanismo telematico in cui l'evoluzione del rapporto contrattuale è funzionale ad un'esecuzione automatizzata di codici e dati informatici. Dunque, nella seconda parte del contributo, il contributo si soffermerà sull'analisi degli effetti patologici di questa nuova programmazione negoziale, alla luce della matrice transnazionale dei contratti fondati su meccanismi informatici.

In particolare, un profilo problematico fondamentale attiene alla natura degli smart contract, in quanto il contesto in cui tale fattispecie negoziale viene elaborata, pattuita ed eseguita determina criticità non solo in ordine all'autodeterminazione negoziale e alla legge disciplinatrice del singolo contratto stipulato, ma anche alla c.d. giurisdizione decentralizzata, da cui derivano possibili criticità in riferimento alla legge applicabile.

Questo scenario, caratterizzato dalla progressiva creazione di una piattaforma negoziale informatica, parallela alla realtà oggettiva, implica un regime giuridico rafforzato a tutela dei contraenti, da cui deriva l'individuazione dei c.d. *digital rights*.

*Contractual self-determination, artificial intelligence and human rights: the construction of dematerialised will*

The evolution of technology, through the implementation of cryptographic mechanisms and algorithms, has inevitably invaded the contractual sphere, influencing not only the willingness to negotiate, but also the concrete role of the parties in pursuing their mutual interests. Furthermore, the effects of automation on contractual programming imply a plurality of pathological profiles in terms of the distinction between human action and virtual subjectivity.
The aim of this contribution is, first and foremost, to identify the progressive dematerialization of the willingness to negotiate brought about by the advent of so-called new technologies, analyzing the main specific categories in which the informatic structure of a contractual relationship can be configured, with particular reference to so-called smart contracts, a new legal institution heralding a virtual legal ecosystem.
Undoubtedly, the analysis of this new type of contract leads to the emergence of new subjective legal situations that need to be protected, as the automated execution of a "smart" contract can lead to an overstepping of the role of the parties, causing a potential systematic violation of human rights. In fact, the effects of blockchain technology in the context of the constraints between contractors involve the implementation of a telematic mechanism in which the evolution of the contractual relationship is functional to the automated execution of computer codes and data. Therefore, in the second part of this article, the contribution will focus on analyzing the pathological effects of this new type of negotiation, in light of the transnational nature of contracts based on computer mechanisms.
In particular, a fundamental problem concerns the nature of smart contracts, as the context in which this type of agreement is drawn up, agreed upon, and executed raises critical issues not only in terms of contractual self-determination and the law governing the individual contract entered into, but also in terms of so-called decentralized jurisdiction, which may give rise to potential problems with regard to the applicable law.
This scenario, characterized by the progressive creation of an informatic negotiation platform parallel to the objective reality, implies a strengthened legal regime to protect contractors, from which the identification of so-called digital rights derives.

*Ciberspazio e diritto*, vol. 26, n. 80 (2 - 2025), pp. 261-279

# Integrazione Normativa e Governance del Rischio nell'Intelligenza Artificiale: Tra AI Act, GDPR e NIS2

Adriano Bertolino*

Sommario: 1. Premessa. – 2. Tassonomia dei rischi nell'ecosistema IA. – 3. Principali vulnerabilità e minacce nei sistemi di IA. – 4. L'AI Act: approccio basato sul rischio e sicurezza *by design*. – 5. GDPR e IA: la sfida dei modelli generativi e l'*accountability* dei dati. – 6. La Direttiva NIS2 e la resilienza cibernetica delle infrastrutture IA. – 7. Verso una governance integrata: sinergie normative e standard tecnici. – 8. Considerazioni finali.

## 1. *Premessa*

L'avvento dell'intelligenza artificiale come tecnologia pervasiva ha innescato un cambiamento di paradigma che pone nuove sfide regolatorie. In pochi anni l'IA è passata dai laboratori di ricerca all'impiego in settori critici: finanza, sanità, giustizia e persino processi decisionali pubblici (es. CEREBRO). Accanto alle enormi opportunità, questa rivoluzione silenziosa ha messo in luce fragilità strutturali difficili da ignorare. I moderni sistemi di IA non sono più semplici algoritmi, ma ecosistemi complessi in grado di incidere su diritti fondamentali, stabilità sociale e fiducia dei cittadini. L'Unione europea ha risposto a tali sfide con un approccio anticipatorio e comprensivo: tre strumenti normativi – l'AI Act, il GDPR e la Direttiva NIS2 – costruiscono una cornice multilivello che trascende la mera tecnica per abbracciare aspetti etici e di governance.

* L'autore possiede una ventennale esperienza in Privacy, Cybersecurity e AI, ricopre ruoli di *CyberLegal*, *Compliance Officer, Data Protection* e *Cybersecurity Manager* per diverse organizzazioni, specializzato in casi complessi di compliance GDPR e framework di sicurezza per enti pubblici e multinazionali. È stato docente presso l'Università di Milano in master su protezione dati e sicurezza delle informazioni, dove la professione incontra la passione per l'innovazione tecnologica e la compliance normativa. Attivo nella divulgazione della cultura della sicurezza e privacy presso scuole e associazioni no profit, per sensibilizzare le nuove generazioni sui temi della data protection e cybersecurity.

doi 10.53148/CD202502003 

Il messaggio del Legislatore europeo è chiaro: l'IA non può essere lasciata a sé stessa. Per essere davvero al servizio della società, l'IA deve essere regolata, sicura e, soprattutto, responsabile.

In quest'ottica integrata, il presente lavoro analizza come le citate normative si intreccino, quali nuovi rischi emergano dall'uso avanzato di modelli di IA – in particolare i *Large Language Models* (LLM) di ultima generazione – e quali sfide di governance ne derivino. Si adotterà un taglio tecnico-giuridico, evidenziando gli obblighi e i principi chiave di ciascun framework normativo e le rispettive zone di sovrapposizione. Dopo aver delineato una tassonomia dei rischi associati all'IA e le principali vulnerabilità tecniche, verranno esaminate le disposizioni dell'AI Act (ancora in fase di attuazione) relative alla sicurezza *by design* e al modello di regolazione basato sul rischio; a seguire, si affronterà il ruolo del GDPR nella tutela dei dati personali in sistemi di IA (con particolare riguardo alla compliance degli LLM) e infine il contributo della Direttiva NIS2 nel rafforzare la resilienza cibernetica delle infrastrutture che impiegano IA. Una sezione conclusiva proporrà, infine, un quadro di governance integrata del rischio AI, in cui convergono requisiti legali, standard tecnici e prassi organizzative, evidenziando come la fiducia rappresenti l'infrastruttura invisibile ma essenziale per un'IA affidabile e al servizio dell'uomo.

## 2. *Tassonomia dei rischi nell'ecosistema IA*

La valutazione e classificazione dei rischi riveste un ruolo fondamentale per comprendere le esigenze regolatorie in materia di IA. Un contributo significativo proviene dall'*AI Risk Atlas* di *IBM Research*[1], che fornisce una tassonomia strutturata dei rischi legati ai sistemi di intelligenza artificiale. Tale studio evidenzia come l'IA sia esposta a un'ampia gamma di rischi che vanno ben oltre i tradizionali attacchi informatici. In particolare, l'*AI Risk Atlas* identifica quattro categorie principali di rischio in ambito IA:

*i)* "Rischi tecnici", ossia vulnerabilità intrinseche nei modelli di IA dal punto di vista tecnologico, ad esempio la suscettibilità ad attacchi adversariali o l'avvelenamento dei dati di training.

[1] Cfr. F. Bagehorn, et al., *AI Risk Atlas: Taxonomy and Tooling for Navigating AI Risks and Resources*, 2025, disponibile al link https://arxiv.org/abs/2503.05780.

*Integrazione Normativa e Governance del Rischio nell'Intelligenza Artificiale: Tra AI Act, GDPR e NIS2*

Il presente lavoro analizza l'ecosistema normativo integrato che disciplina l'intelligenza artificiale (IA) nell'Unione europea, esaminando in particolare l'intersezione tra il Regolamento sull'IA (AI Act), il Regolamento Generale sulla Protezione dei Dati (GDPR) e la Direttiva NIS2 in materia di cybersecurity. Viene adottato un approccio tecnico-giuridico per evidenziare come tali strumenti normativi, seppur differenti per ambito, concorrano a una governance unitaria del rischio digitale. Dopo un'introduzione sul mutato panorama tecnologico, si esaminano le categorie di rischio dell'IA – da vulnerabilità tecniche a rischi etici – e le principali minacce specifiche (attacchi adversariali, *data poisoning*, *model inversion*, *model stealing*). Si approfondiscono quindi le previsioni dell'AI Act in tema di *security by design* e gestione del ciclo di vita dei sistemi ad alto rischio, le sfide poste dagli algoritmi generativi rispetto al GDPR (memorizzazione di dati personali nei modelli di IA, principi di minimizzazione e obblighi di *accountability*), nonché i requisiti di resilienza operativa e notifica incidenti introdotti dalla Direttiva NIS2. Viene infine proposta una visione di governance integrata, che richiede sinergia tra compliance normativa, misure di sicurezza tecnico-organizzative e *accountability* etica, al fine di costruire un'infrastruttura invisibile di fiducia nell'IA a beneficio di innovazione e tutela dei diritti.

*Regulatory Integration and Risk Governance in Artificial Intelligence: Between the AI Act, GDPR, and NIS2*

This paper examines the integrated regulatory ecosystem governing Artificial Intelligence (AI) in the European Union, focusing on the interplay between the Artificial Intelligence Act (AI Act), the General Data Protection Regulation (GDPR), and the NIS2 Directive on cybersecurity. Adopting a highly technical-legal approach, the analysis highlights how these instruments, despite differing scopes, collectively contribute to a unified governance of digital risk. After introducing the paradigm shift in AI deployment, the paper explores AI risk categories – from technical vulnerabilities to ethical risks – and key AI-specific threats (adversarial attacks, data poisoning, model inversion, model stealing). It then delves into the AI Act's provisions on security by design and lifecycle risk management for high-risk systems, the challenges posed by generative algorithms under the GDPR framework (e.g., AI models memorizing personal data, the principles of data minimization and accountability), as well as the operational resilience and incident notification requirements under the NIS2 Directive. Finally,

a vision for integrated AI governance is proposed, calling for synergy between legal compliance, technical-organizational security measures, and ethical accountability, with the aim of building an invisible infrastructure of trust in AI that balances innovation with the protection of rights.

*Ciberspazio e diritto*, vol. 26, n. 80 (2 - 2025), pp. 281-294

# La proposta di un nuovo diritto alla *cybersecurity*: alcune considerazioni fra aspetti antropologici e giuridici

Emanuele Brambilla*

Sommario: 1. La cybersecurity nelle sue dimensioni giuridiche e antropologiche. – 2. Un nuovo diritto alla cibersicurezza? Alcune problematiche. – 3. Alcune possibili risposte. – 3.1. L'aporia contenutistica. – 3.2. L'aporia della sovrapposizione. – 3.3. L'aporia dell'armonizzazione.

## 1. *La cybersecurity nelle sue dimensioni giuridiche e antropologiche*

Nell'odierna società digitale, la *cybersecurity*, solitamente interpretata come l'insieme delle misure tecniche volte a prevenire, minimizzare e contrastare attacchi informatici, diviene altresì una delle componenti sostanziali della protezione dell'"immagine" digitale degli utenti[1]. Infatti, alla sicurezza e alla resilienza di un sistema non si contribuisce semplicemente attraverso misure di stampo tecnico-informatico, ma anche grazie all'importanza dei comportamenti individuali e alla salvaguardia delle condizioni stesse che permettono l'esercizio dei diritti digitali e la fiducia nei sistemi.

* Dottorando in Filosofia del diritto presso il Dipartimento di Scienze giuridiche "Cesare Beccaria" dell'Università degli Studi di Milano e Research Fellow presso l'*Information Society Law Centre* (ISLC).

[1] Va ricordato che la definizione stessa del termine è stata molto discussa e presenta notevoli sfumature. Sul tema, si consulti il seguente articolo dove vengono presentate ventinove definizioni elaborate da differenti studiosi o enti dal 2009 al 2016: D. Schatz, R. Bashroush, J. Wall, "Towards a More Representative Definition of Cyber Security", «Journal of Digital Forensics, Security and Law», vol. 12, n. 2, 2017, pp. 53-74; d'altro canto, anche l'ENISA ritiene che sia un termine composito e che, conseguentemente, non sia necessario trovarne una definizione precisa in quanto «*is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers*». ENISA, *Definition of Cybersecurity. Gaps and Overlaps in Standardisation*, dicembre 2015, https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf, p. 28 (11/09/25).

A tal proposito, alcuni studiosi propongono una distinzione semantica fra cibersicurezza come "prassi" e cibersicurezza come "stato". Il primo termine, come già si può evincere dal nome, si riferisce agli aspetti tecnici della sicurezza informatica, ossia a tutte quelle misure volte a rendere un sistema resistente e sufficientemente protetto. A questo scopo, contribuiscono sia le organizzazioni che si occupano di cibersicurezza sia gli utenti stessi, che lungi dall'essere dei destinatari passivi, sono chiamati a partecipare alla creazione di un ambiente digitale resiliente. La sicurezza informatica come stato, invece, è conseguibile soltanto se questo primo stadio viene adeguatamente raggiunto e compreso. Infatti, uno "stato" di cibersicurezza è veramente tale quando "le persone naturali e legali" sono protette contro le minacce cibernetiche e quando si sentono sicure e desiderano continuare ad esserlo[2]. Il mantenimento di tale stato, inoltre, non dipende soltanto dalla robustezza delle infrastrutture critiche, ma altresì da una proporzionata allocazione degli oneri a capo dei beneficiari e di tutti i soggetti coinvolti.

Per queste ragioni, si potrebbe paragonare la sicurezza informatica ad una sorta di "virtù collettiva", ossia all'insieme di disposizioni e pratiche condivise che, unendo singoli utenti e organismi specializzati, sono in grado di orientare decisioni e modi di agire. Detto altrimenti, la virtù collettiva è, pur nella diversità di ruoli e capacità di *governance* o collaborazione, una stabile e duratura unione di intenti verso un obbiettivo

[2] «Cybersecurity as praxis would then be understood as the activities and measures to accomplish cybersecurity's aims and objectives. It would include a requirement to act, to undertake concrete actions. Accordingly, cybersecurity as a state would mean the condition that is achieved once cybersecurity as praxis has succeeded; within cybersecurity as a state natural and legal persons need to be protected against any cyber threat. Within its protective sphere natural and legal persons need to be (cyber)secure, to have a claim to remain so and for others to respect their wish […] cybersecurity as praxis could conceptually either include everybody or pertain only to a few. Under a participatory approach everybody would somehow need to act or carry out measures: individuals and legal persons would have to take action, as prescribed by law or other regulations, in order for each to contribute proportionately to achieving the cybersecurity aims». Cfr. V. Papakonstantinou, "Cybersecurity as Praxis and as a State: the EU Law Path Towards Acknowledgement of a New Right to Cybersecurity?", «Computer Law & Security Review», vol. 44, 2022, pp. 2-5.

*La proposta di un nuovo diritto alla* cybersecurity: *alcune considerazioni fra aspetti antropologici e giuridici*

La *cybersecurity*, sebbene richieda misure tecniche concrete per fronteggiare le sempre più multiformi minacce informatiche, presenta anche una forte componente antropologica e giuridica. Il presente contributo, dopo aver specificato il valore di queste due componenti con speciale attenzione a quella antropologica, mira ad analizzare la possibile introduzione di un diritto alla cibersicurezza. Per fare questo, prende in esame tre differenti, ma convergenti, problematiche in relazione all'eventualità di tale introduzione, mostrando come sia necessaria una loro previa risoluzione. In seguito, l'articolo tenta di dare una possibile risposta a questi tre interrogativi, mostrando come la via da percorrere per una formulazione compiuta di questo diritto, sebbene già avviata, richieda ulteriori riflessioni per evitare di creare sovrastrutture troppo complesse che inficino l'esercizio di altri diritti affini. Infine, si suggeriscono dei possibili "luoghi giuridici" in cui poterlo inserire dal punto di vista teorico-normativo.

*The proposal of a new right to cybersecurity: few considerations between anthropological and juridical aspects*

Cybersecurity is often presented as a set of concrete technical measures that helps facing increasingly multifaceted threats. However, it is also particularly characterized by profound anthropological and legal dimensions. The article, after clarifying the significance of both aspects, with particular emphasis on the former, examines the possible recognition of a right to cybersecurity. To achieve this goal, it addresses three distinct yet convergent questions that must be solved as prerequisites for such recognition. Afterwards, it tries to formulate an answer to these three problems, taking into consideration that, even if the path to this kind of formulation is already in progress, it needs further reflections to avoid the creation of superstructures that could hinder other rights. The analysis ends with theoretical and normative suggestions on plausible "legal *loci*" in which this new right could be included.