Giorgia Bevilacqua è Ricercatrice di Diritto internazionale presso il Dipartimento di Giurisprudenza dell'Università degli Studi della Campania Luigi Vanvitelli. Ha pubblicato numerosi contributi scientifici in materia di diritto del mare, sport, sicurezza e tutela dei diritti umani. È stata responsabile di unità del progetto *SecCo-OC* e ha coordinato e partecipato a vari progetti di ricerca di rilevanza scientifica nazionale e internazionale.

Veronica Caporrino è Professoressa associata di Diritto privato comparato presso il Dipartimento di Giurisprudenza dell'Università degli Studi della Campania Luigi Vanvitelli. È autrice di due monografie nonché di numerosi saggi, contributi in opere collettanee e lavori minori.

Federica De Simone è stata Ricercatrice di tipologia A in Diritto penale sino al 2024 presso il Dipartimento di Giurisprudenza dell'Università degli Studi della Campania Luigi Vanvitelli. È autrice e curatrice di numerosi contributi scientifici anche in lingua inglese e di due monografie: *Nuove coordinate in tema di prevenzione e contrasto della corruzione* (2025) e *La sanzione detentiva. Dal modello securitario al modello trattamentale* (2018).

Carmen Di Carluccio è Professoressa associata di Diritto del lavoro presso il Dipartimento di Giurisprudenza dell'Università degli Studi della Campania Luigi Vanvitelli. È autrice e curatrice di numerose pubblicazioni scientifiche, anche in lingua spagnola e inglese. Per i nostri tipi è autrice della monografia *Lavoro e salute mentale dentro e fuori l'istituzione* (2022).

euro 30

This volume presents the results of a study conducted by a research unit at the University of Campania Luigi Vanvitelli as part of the *SecCo-OC Secure Containers Open Call* project, which is dedicated to the development of advanced cybersecurity models for digital platforms and applications. In a context where technology is becoming increasingly intertwined with everyday life, this work offers a systematic analysis of the key challenges raised by the digital transition.

Through an interdisciplinary study, the epistemological categories of law are examined in relation to the use of new technologies, starting with the issue of the dematerialisation of legal assets, the security of digital infrastructure and the governance of platforms, and extending to the problem of algorithmic management of work and the preservation of general principles and fundamental rights. The study is conducted from a multi-level perspective, taking into account the international, EU and domestic frameworks.

Organised into four sections dedicated to the geopolitical dimension of cybersecurity, European digital governance, the impact of emerging technologies on private law, and the transformations of work in the age of algorithms, the volume provides a detailed yet coherent picture of the challenges posed by innovation. Taken together, the contributions highlight the need to rethink the categories, instruments and functions of law within the contemporary digital ecosystem. This gives rise to a conception of the legal system called upon to actively govern technological development, ensuring its compliance with fundamental guarantees and preventing the emergence of new forms of vulnerability.

The work is intended as a tool for in-depth analysis and critical reflection, contributing to the debate on the definition of a regulatory paradigm capable of combining innovation, security and the protection of human dignity and democratic values.

ISBN 979-12-235-0543-4

SECURITY AND RIGHTS IN CYBERSPACE

ESI

SECURITY AND RIGHTS IN CYBERSPACE

Interdisciplinary Insights from the SecCo-OC European Research Project

a cura di
Giorgia Bevilacqua
Veronica Caporrino
Federica De Simone
Carmen Di Carluccio

grale spin-off universitario
Università degli Studi della Campania Luigi Vanvitelli

DIRITTO INNOVAZIONE E SOCIETÀ
COLLANA DEL G.R.A.L.E. SPIN OFF UNIVERSITARIO
DIPARTIMENTO DI GIURISPRUDENZA
UNIVERSITÀ DEGLI STUDI
DELLA CAMPANIA LUIGI VANVITELLI

SAGGI

Editoriale Scientifica

Diritto, Innovazione e Società è una Collana di volumi che trae origine dall'esperienza del G.R.A.L.E. Spin off del Dipartimento di Giurisprudenza dell'Università della Campania Luigi Vanvitelli. Essa si fonda sulla combinazione tra l'indagine scientifica e l'elaborazione teorica, con l'intento di offrire uno spazio di riflessione e confronto aperto, capace di accogliere stimoli e prospettive differenti. Il titolo scelto per la Collana, volutamente ampio, riflette la consapevolezza che la ricerca giuridica non può essere circoscritta nei confini di un singolo settore disciplinare, ma necessita del dialogo con altre aree del sapere. L'obiettivo è favorire approcci trasversali in grado di affrontare la complessità del mondo contemporaneo, dalle questioni strettamente giuridiche alle sfide più generali poste dall'innovazione tecnologica, economica e sociale. Con questo proposito, *Diritto, Innovazione e Società* aspira ad accogliere contributi provenienti non solo dall'ambito giuridico in senso stretto, ma anche da discipline affini o complementari, così come da ricerche redatte in lingua straniera, nella convinzione che l'incontro tra punti di vista diversi arricchisca il dibattito e favorisca lo sviluppo di una cultura scientifica autenticamente interdisciplinare.

DIRITTO, INNOVAZIONE e SOCIETÀ

DIRITTO, INNOVAZIONE e SOCIETÀ
Collana del G.R.A.L.E. Spin off Universitario
Dipartimento di Giurisprudenza, Università degli Studi della Campania Luigi Vanvitelli

Sez. I – ***Saggi***

SECURITY AND RIGHTS IN CYBERSPACE

Interdisciplinary Insights from the SecCo-OC European Research Project

a cura di

Giorgia Bevilacqua
Veronica Caporrino
Federica De Simone
Carmen Di Carluccio

Editoriale Scientifica

Pubblicazione realizzata nel quadro del progetto *SecCo-OC. Secure Containers Open Call*, inserito nel più ampio progetto *SecCO* (Secure Containers). L'iniziativa si colloca nel contesto dei bandi a cascata promossi dalla Fondazione SERICS-Security and Rights in the CyberSpace, soggetto attuatore del Partenariato esteso "Cybersecurity, nuove tecnologie e tutela dei diritti", previsto dal Piano Nazionale di Ripresa e Resilienza (PNRR).

I contributi accolti nel Volume sono stati sottoposti a referaggio anonimo a doppio cieco.

via San Biagio dei Librai, 39 - 80138 Napoli
www.editorialescientifica.com info@editorialescientifica.com
ISBN 979-12-235-0543-4

Indice

EU DIGITAL GOVERNANCE, DIGITAL IDENTITY, DATA AND FUNDAMENTAL RIGHTS

EMERGING TECHNOLOGIES AND THE EVOLUTION OF PRIVATE LAW

ALGORITHMS, WORK AND NEW SOCIAL RIGHTS IN THE DIGITAL ERA

PREFAZIONE

Massimiliano Rak

Questo volume nasce nell'ambito del progetto *SecCo-OC. Secure Containers Open Call*, inserito nel più ampio progetto *SecCO (Secure Containers)*. L'iniziativa si colloca nel contesto dei bandi a cascata promossi dalla Fondazione *SERICS-Security and Rights in the CyberSpace*, soggetto attuatore del Partenariato esteso "Cybersecurity, nuove tecnologie e tutela dei diritti", previsto dal Piano Nazionale di Ripresa e Resilienza (PNRR).

Il Progetto si propone un obiettivo scientifico ben definito: sviluppare nuove metodologie per la progettazione e realizzazione di applicazioni a microservizi, basate sulla tecnologia dei container, nel rispetto di stringenti requisiti di cybersecurity. L'ambito di ricerca è dunque prevalentemente informatico, con particolare riferimento ai temi dell'ingegneria del software e della sicurezza dei sistemi.

Ho contribuito alla definizione del progetto sin dalle sue fasi iniziali, in qualità di esperto di cybersecurity, ricoprendo inizialmente anche i ruoli di vicecoordinatore del progetto e di coordinatore dell'unità di ricerca. In tale contesto, la mia attività si è concentrata sullo sviluppo di approcci volti all'automatizzazione dei processi di valutazione della sicurezza di applicazioni e infrastrutture. L'obiettivo è quello di individuare tecniche che, con un intervento limitato da parte di esperti, consentano di evidenziare vulnerabilità, punti deboli e minacce nei sistemi in fase di sviluppo. Tali metodologie si fondano su una modellazione del sistema e, in particolare, dei requisiti di sicurezza dei singoli componenti – i container che implementano i microservizi – attraverso i cosiddetti Security Service Level Agreement (Security SLA), strumenti che definiscono il livello minimo di sicurezza richiesto a ciascun componente.

Tuttavia, la sicurezza informatica non può essere considerata un problema esclusivamente tecnico. Le garanzie richieste non si esauri-

scono nelle contromisure tecnologiche, ma comprendono profili organizzativi, l'attribuzione delle responsabilità, la tracciabilità delle azioni e la valutazione sistematica dei rischi. Tale dimensione trasversale trova oggi riscontro in un quadro normativo sempre più articolato, che include, tra gli altri, il GDPR (General Data Protection Regulation), la direttiva NIS e la più recente NIS 2, nonché il Cybersecurity Act e il Cyber Resilience Act.

A partire da queste considerazioni è maturata l'idea di ampliare il gruppo di ricerca inizialmente coinvolto nel progetto, composto esclusivamente da ingegneri informatici, includendo competenze giuridiche in grado di analizzare le implicazioni normative connesse allo sviluppo di sistemi sicuri.

Successivamente, a seguito del mio trasferimento presso un diverso gruppo di ricerca – pur rimanendo coinvolto nel progetto – il coordinamento dell'unità è stato affidato al gruppo del Dipartimento di Giurisprudenza. Questo passaggio ha favorito un'evoluzione significativa delle attività di ricerca: l'unità ha progressivamente acquisito piena autonomia, orientandosi in modo sempre più deciso verso l'analisi giuridica della cybersecurity e delle sue implicazioni.

Da questa linea di ricerca prendono forma i contributi raccolti nel presente volume, che offrono prospettive diverse – talvolta anche tra loro eterogenee – sui problemi giuridici connessi alla crescente diffusione delle tecnologie informatiche. Essi mettono in luce, in particolare, la necessità di sviluppare nuovi strumenti normativi o di adattare quelli esistenti a contesti tecnologici in continua evoluzione.

Il volume non ambisce a fornire una trattazione esaustiva di un tema così ampio e complesso, ma intende offrire una selezione di contributi che affrontano specifiche questioni con un approccio rigoroso e consapevole della natura interdisciplinare della materia. La lettura di questi saggi – così come il confronto con i colleghi che li hanno elaborati – ha rappresentato per me un'importante occasione di approfondimento, consentendomi di ampliare la prospettiva su problematiche che, se considerate esclusivamente in chiave tecnico-ingegneristica, rischiano di rimanere in secondo piano.

Per tali ragioni, ritengo che il volume costituisca uno strumento di interesse sia per gli studiosi del diritto, che potranno individuare nuovi ambiti di ricerca in un settore particolarmente dinamico, sia per i ricercatori e i professionisti in ambito tecnico, interessati a comprendere più a fondo le implicazioni normative delle proprie attività.

THE INVISIBLE FABRIC OF DIGITAL TECHNOLOGIES: LEGAL PATHWAYS AMID THREATS AND CHALLENGES. FINDINGS AND OUTLOOKS FROM RESEARCH CONDUCTED IN THE *SecCo-OC PROJECT*

*Giorgia Bevilacqua e Carmen Di Carluccio**

1. Day after day, technology is making its way into our daily lives. Tiny devices open our eyes as we wake, warm our homes, our offices and, at times, even our hearts with the same natural ease. An invisible army of apps makes it possible to order groceries, book a taxi or a parking space, buy a ticket for a musical or a theatre show, or arrange a doctor's appointment. Technology simplifies our lives, to the point of taking over many of our tasks. It recognises people and objects, translates and reads aloud short texts and long manuscripts. Autonomous or semi-autonomous vehicles can quietly move us between airport terminals or across city points, depending on local regulations.

All this – and much more – is made possible by the invaluable work of computer science researchers involved in scientific research projects such as *SecCo-OC. Secure Containers Open Call*[1], from which this collection of contributions originates. This project aims to develop and consolidate innovative technologies in the field of cybersecurity, establishing theoretical and practical models for the analysis, management and regulation of issues relating to the security of digital platforms and applications.

* This paper is the result of a shared reflection; however, § 2 and 3 were written by Giorgia Bevilacqua, while § 4 and 5 were written by Carmen Di Carluccio. § 1 and 6 were drafted together by both Authors.

[1] The *SecCo-OC. Secure Containers Open Call* project forms part of the wider *SecCO (Secure Containers)* project. The initiative takes place within the framework of the cascading calls for proposals promoted by the SERICS Foundation - *Security and Rights in the CyberSpace*, the implementing body of the extended partnership "Cybersecurity, new technologies and the protection of rights", as provided for in the National Recovery and Resilience Plan (PNRR).

We legal professionals, too, have turned our attention to the technological innovation that is bursting into everyone's lives; therefore, driven by the ambition, or at least the desire, to contribute to this research, we have considered how to make digital platforms and applications more secure from a legal perspective. We, thus, set the study in motion by first familiarising ourselves with these new digital tools with the support of our project colleagues who are experts in the hard sciences. Having filled this knowledge gap, we shifted the focus of our investigation to contexts more familiar to us, conducting a survey of the regulations that already exist or are still lacking at international and supranational levels and within various national legal systems (see appendices – mapping).

It is from this collaborative process – technical, legal and interdisciplinary – that this volume has emerged. The four sections that follow examine, from different yet complementary perspectives, the main challenges posed by the digital transformation: the geopolitical and international dimensions of cybersecurity; European digital governance and the protection of fundamental rights; the impact of emerging technologies on areas of private law; and the transformation of work in the age of algorithms and new digital social rights. Each section brings together contributions that engage with one another, forming a complex yet coherent mosaic capable of conveying the depth of the changes underway and the need for a legal framework that can accompany, govern and, at times, contain technological innovation.

2. The first section of the volume addresses the broader, structural level of digital transformations: the realm where technology, public power and global security intertwine, redefining the boundaries of sovereignty and the international protection of human rights. In this hybrid space – where algorithms, data and digital infrastructure become tools of governance, surveillance and even conflict – international law is called upon to grapple with unprecedented forms of the exercise of power and with new individual and collective vulnerabilities. The contributions collected here offer a detailed analysis of these phenomena, demonstrating how technology is not merely an operational tool, but

a political and legal factor capable of profoundly influencing the structure of international relations.

The first essay analyses the case of the so-called "Celestial Empire of China", demonstrating how technology can become a genuine instrument of social control. The author highlights the paradigm shift from an *ex post* control model, based on the detection of wrongdoing, to *ex ante* control, based on the statistical prediction of behaviour. On the premise, therefore, that algorithms, big data and artificial intelligence represent a new form of governance, founded on the management of populations through data, the article sheds light on the progressive opacity of Chinese public decisions entrusted to indecipherable formulas that are capable of openly undermining that quality of law which international law requires as a condition for the legitimacy of state interference in fundamental rights.

The second contribution addresses the equally sensitive issue of covert mass surveillance carried out through spyware and tools originally designed for military or governmental purposes, which subsequently end up being used by private individuals for clearly unlawful ends. The author examines the legitimacy of the use of such technologies within the framework of international human rights protection mechanisms, with the aim of identifying conditions, limits and safeguards that allow for a balance between security requirements and the protection of fundamental freedoms.

The third essay focuses on hybrid conflicts, namely those conflicts waged not only with bombs and missiles – traditional weapons – but also with a range of modern, advanced technological tools and, consequently, with a series of cyber operations capable of inflicting devastating consequences on the infrastructure of the targeted State. From the perspective of an international lawyer, an individual's cyber security is, in fact, relevant both in times of peace and in times of war. The author analyses the conditions for the applicability of international norms, highlighting the persistent interpretative uncertainties despite the attempts at clarification offered by the Tallinn Manual 2.0. The paper aims to ascertain when an attack launched against a State's critical infrastructure triggers the application of the customary rule prohibiting

the use of force, as well as when an attack carried out by one or more individuals can be formally attributed to a State.

The section concludes with a contribution on criminal law that addresses the tensions generated by the dematerialisation of property and the transition from *res corporalis* to *res digitalis*. The author demonstrates how the current digital ecosystem is undermining the traditional categories of property offences, highlighting the limitations of equating a computer file with a 'movable object' – an approach attempted by case law – and the consequent difficulties in defining concepts such as theft or dispossession without undermining the principle of legality. Hence the need to resort to distinct offences, such as computer fraud, which shifts the focus from the deception of human will to the technical manipulation of the system. The essay clarifies the dividing line between fraud and computer fraud, particularly with regard to contemporary phenomena such as cheating and social engineering, and highlights the persistent gaps in protection in cases where digital damage does not have immediate financial implications.

These essays show that cyberspace geopolitics is a tangible space where sovereignty, security, and rights are being redefined. Technological transformations affect both the dynamics of public power and more traditional categories of criminal law, highlighting the need for legal instruments capable of addressing intangible assets, hybrid attacks and new forms of individual and collective vulnerability. Understanding these dynamics is the first step towards building a digital ecosystem that is not only efficient and innovative, but also fair, transparent and respectful of human dignity.

3. The second section of the volume looks at the heart of the legal transformations triggered by European digitalisation: the creation of a governance ecosystem capable of integrating technological innovation, the protection of fundamental rights and the security of digital infrastructure. Digital identity, cyber resilience, cross-border data transfers and digital health represent four critical junctures in this transition, where the Union's and Member States' ability to govern the complexity of cyberspace without sacrificing inclusion, personal protection and the coherence of the regulatory framework is put to the test.

The first contribution analyses the human rights implications arising from the national implementation of the European Digital Identity (EUDI). Through a comparison of various European models and a focus on Romania, the author highlights how structural inequalities – regional disparities, insufficient digital skills, and a lack of assistive technologies – can undermine the effectiveness of a truly universal digital identity. The analysis shows that the EUDI's promise of interoperability and accessibility requires active public policies, inclusion tools and independent mechanisms for monitoring rights.

The second essay explores the relationship between cybersecurity and the right to personal data protection, taking as its starting point the idea that the security of digital infrastructure is an essential prerequisite for the effectiveness of the right to privacy. The author traces the evolution of European cybersecurity regulation, questioning the ability of the most recent initiatives – from the NIS 2 Directive to the Cyber Resilience Act – to provide a harmonised response to the systemic risks threatening digital networks and services. From this perspective, cybersecurity is interpreted as a necessary condition for the lawful and compliant processing of personal data, highlighting how clearer and more uniform technical standards can strengthen both *ex ante* measures and *ex post* safeguards. Particular attention is paid to the potential role of Annex I of the Cyber Resilience Act in defining the scope of Article 32 of the GDPR, helping to reduce grey areas of responsibility for data controllers and to raise the overall level of security. The conclusions emphasise the need for an interdisciplinary and systemic approach capable of integrating the various regulatory sources and promoting effective protection of the right to personal data protection within the European digital ecosystem.

The third contribution addresses the crucial and increasingly controversial issue of the transfer of personal data to third countries, with particular attention to the relationship between the European Union and the United States. The author examines the balance between security requirements and the protection of privacy, focusing on the critical issues generated by the globalisation of information flows and the widespread use of technologies such as e-commerce, cloud computing

and social networks. The Data Privacy Framework emerges not only as a central hub for the protection of data subjects' rights, but also as a source of tension regarding the GDPR's control, accountability and enforcement mechanisms within the US context.

The fourth essay focuses on the protection of personal data in digital healthcare, with particular reference to telemedicine. The analysis highlights how the digitisation of healthcare services, whilst offering significant opportunities, amplifies the risks associated with data quality, data security and the possibility of unauthorised access. Privacy in the healthcare sector, traditionally rooted in the principle of confidentiality and professional secrecy, takes on new dimensions in the context of e-health, prompting a rethinking of the safeguards protecting sensitive data and personal dignity.

The various contributions demonstrate that European digital governance cannot be reduced to a set of technical or regulatory tools, but must be interpreted as a political and legal project that directly impacts citizenship, substantive equality and the protection of fundamental rights in the digital age.

4. The third section of the volume examines one of the most dynamic and challenging areas of contemporary law: the impact of emerging technologies on the structure, categories and functions of private law. Blockchain, virtual property, digital ecosystems in the fashion industry and new reproductive technologies are fields that are only seemingly distant. In reality, they share the same evolutionary trajectory in which technological innovation challenges traditional concepts – property, liability, identity, corporeality – and pushes for a rethinking of established legal paradigms.

The first contribution analyses Decentralised Autonomous Organisations (DAOs), an organisational form native to blockchain that combines automation, algorithmic governance and smart contracts. The author highlights how the promise of transparency and decentralisation is accompanied by profound vulnerabilities: coding flaws, reentrancy risks, arithmetic errors and weaknesses in accessing control mechanisms can compromise the integrity of funds and the stability

of the organisation. Added to this are the risks of governance manipulation, including the possibility of acquiring a majority control of decision-making tokens. DAOs thus emerge as a prime laboratory for observing the tension between automation and legal liability.

The second essay examines trademark protection in digital fashion, highlighting how digitalisation increases both opportunities and risks. Phenomena such as cybersquatting, the immediate replicability of distinctive signs and the globalisation of digital markets are putting pressure on traditional protection mechanisms. Through a comparative approach, the author demonstrates how brand protection can no longer be conceived solely as a defence of the enterprise's economic identity, but must be integrated with the protection of internet users and the need to rethink the rules in a competitive and dematerialised environment.

The third contribution explores a radically different yet equally emblematic area of the transformation of private law: advanced reproductive technologies, with particular attention to artificial wombs. A comparison between the United States and France highlights how legal systems oscillate between openness and caution in the face of techniques that redefine the very concept of birth, raising questions about parental responsibility, the legal status of the artificial foetus, and the limits of technological intervention in the human body. This analysis demonstrates how biotechnological innovation directly challenges fundamental categories of personal and family law.

The section concludes with a contribution dedicated to virtual property, which analyses the Georgian case as a paradigmatic example of the difficulties legal systems face in recognising and regulating digital assets of growing economic and social value. Through an examination of comparative doctrine and case law – including the well-known decision of the Bonn Regional Court on virtuelles Eigentum – the authors identify the structural elements of virtual property and demonstrate how the Georgian legal framework, limited to traditional intangible assets, is inadequate for regulating resources such as domain names, virtual environments, digital files and crypto-assets. This highlights the need for a systematic evolution that adapts the classical principles of property to the specific characteristics of the digital environment.

Taken as a whole, the contributions in this section reveal that emerging technologies do not merely introduce new legal objects, but call for a profound revision of the categories of private law, which must now grapple with unprecedented forms of value, identity, corporeality and governance. It is in this dialogue between innovation and tradition that the law's ability to remain an effective instrument of regulation and protection in the digital age is at stake.

5. The fourth section of the volume examines one of the most sensitive issues surrounding digitalisation: the impact of artificial intelligence and digital platforms on employment relationships and the protection of social rights. The automation of decision-making processes, algorithmic workforce management, the emergence of new forms of vulnerability and the spread of atypical employment models outline a context in which labour law is called upon to redefine its instruments, categories and fundamental safeguards. The contributions gathered here offer a detailed analysis of this transition, highlighting how technological innovation is a structural factor affecting the dignity, equality, safety and health of workers.

The first essay explores algorithmic transparency as a new fundamental right in cyberspace. The author highlights how, in digital work, transparency is not a technical feature but an essential legal guarantee for understanding and challenging automated decisions that affect recruitment, performance reviews, task assignments and dismissals. Through a critical analysis of the GDPR, the AI Act and the Platform Work Directive, it becomes clear that formal information is not enough: without access to the decision-making logic, there can be no effective protection or safeguarding of human dignity in the digital workplace.

The second contribution focuses on the issue of algorithmic accountability, outlining a new body of digital workers' rights based on the prevention of automated discrimination. Information, access, explanation, human intervention and trade union oversight become indispensable tools for reducing information asymmetry and ensuring traceability and accountability in algorithmic decisions. The author proposes a multi-level model of accountability – individual, collective

and institutional – that integrates anti-discrimination law, data protection and labour law, outlining an innovative paradigm of substantive equality in the digital environment.

The third essay analyses the limits on the use of artificial intelligence in employment relationships in light of Regulation (EU) 2024/1689. Through a comparative approach, the author demonstrates how many applications used in human resources management – from recruitment to performance appraisal, right through to termination of employment – fall into the high-risk category. This analysis highlights the need for adequate training, qualified human supervision and accurate assessments of the systems' impact within a regulatory context that is still evolving and characterised by limited specialist literature.

The fourth contribution, with reference to the Spanish legal system, examines the growing role of algorithms in employment relationships and the challenges they pose for legal regulation. The author analyses the use of algorithms as tools for decision-making, staff selection, the exercise of managerial power and the monitoring of work activities, emphasising the need for a regulatory framework that reconciles technological innovation, the protection of fundamental rights and the safeguarding of trade secrets. Particular attention is paid to the role of collective bargaining, which is called upon to manage a change that requires a renewed 'natural intelligence' to address the challenges of artificial intelligence.

The fifth essay broadens the perspective, addressing the issue of children's presence in digital environments and new forms of work involving children and adolescents. The essay highlights how online technologies offer educational and creative opportunities, yet expose children to significant risks, particularly when the digital sphere becomes a space for content creation and work. Baby influencers, content creators and minors active on platforms operate in the absence of an adequate regulatory framework, with repercussions on their mental and physical health, privacy and protection from exploitation, surveillance and addiction. The essay emphasises the need for comprehensive regulatory intervention that recognises the specific nature of children's digital work and introduces effective preventive and protective measures.

The section concludes with a contribution dedicated to fixed-term employment contracts within the European Union. The author analyses the evolution of legislation and case law relating to atypical forms of work, highlighting how the flexibility demanded by the contemporary labour market must be balanced by adequate guarantees of security and equal treatment. By examining Directive 1999/70/EC, the case law of the Court of Justice and the Romanian transposition legislation, this essay demonstrates how fixed-term employment constitutes a structurally precarious form of work that requires active policies and social protection measures capable of addressing the new vulnerabilities of digital and non-standard work.

Viewed as a whole, the contributions in this section offer a comprehensive picture of a rapidly changing landscape in which artificial intelligence, digital platforms and new forms of work are redefining rights, safeguards and responsibilities. In such a scenario, it becomes essential to ensure that the individual remains at the centre and to guarantee conditions of transparency, fairness, security and respect for dignity.

6. Taken together, the reflections presented here allow us to grasp the scale of the transformations that technological innovation is imposing on the various legal systems examined, highlighting issues that span different fields but converge on the need to rethink the categories, instruments and functions of the law in the digital age. It is within this framework that the volume as a whole is situated. The contributions gathered here arise from the gathering of diverse expertise and a shared commitment to rigorously and thoroughly examining the legal implications of the technological processes currently underway. Despite the diversity of approaches, they form a complex yet coherent mosaic that captures the intricacy of the contemporary digital landscape and the challenges it poses to the protection of rights, security and legal regulations. What emerges is the conviction that the law must not merely record the changes brought about by digital technologies, but must assume a role in guiding, governing and, where necessary, restraining innovation, so that it remains consistent with the fundamental values of the individual, the community and democratic institutions. Only

a regulatory framework capable of fulfilling this role can ensure that technological development translates into an effective strengthening of safeguards rather than new forms of vulnerability.

It is in this spirit that this volume begins: an invitation to critically examine the transformations underway and to continue a dialogue which, like any evolutionary process, is destined to develop over time, guiding legal systems in defining new forms of protection and governance of technology.

To conclude these introductory notes, the editors of this volume wish to express their gratitude to Massimiliano Rak for making this project possible and for the constant scientific and personal support that has accompanied every stage of the work. Equally sincere thanks go to all our colleagues – both Italian and international – who generously accepted the invitation to contribute to this collective reflection. Their willingness to participate, the quality of their studies and the interdisciplinary perspective they have brought to these pages constitute the true added value of this work.

GEOPOLITICS, SECURITY AND FUNDAMENTAL RIGHTS IN CYBERSPACE

IL CELESTE IMPERO TRA SISTEMI TECNOLOGICI DI CONTROLLO SOCIALE E TUTELA DEI DIRITTI FONDAMENTALI

Alessandro Leopizzi

1. Il concetto di controllo sociale costituisce una categoria trasversale, che precede e oltrepassa il diritto positivo. In senso classico, esso indica l'insieme dei meccanismi – giuridici e non giuridici – attraverso i quali una collettività orienta, condiziona o disciplina i comportamenti individuali[1].

Il diritto rappresenta storicamente la forma più formalizzata e istituzionalizzata di controllo sociale, caratterizzata da generalità, astrattezza e sanzionabilità.

Nella prospettiva della teoria generale del diritto, il controllo sociale giuridico si distingue da quello morale, religioso o consuetudinario per almeno tre elementi: la pretesa di validità normativa, il monopolio della coercizione legittima, la mediazione dell'autorità giudiziaria[2].

Tuttavia, il rapporto tra diritto e controllo sociale non è statico. Esso muta al mutare delle tecniche di governo e delle strutture materiali

[1] G. Gurvitch Georges, *Il controllo sociale*, Armando Editore, 1997; N. Bobbio, *Dalla struttura alla funzione: nuovi studi di teoria del diritto*, Laterza, 2014.

[2] Max Weber individua nel monopolio della coercizione legittima uno degli elementi qualificanti dell'ordinamento giuridico moderno: A. De Simone, *Razionalità e diritto in Max Weber*, in *Diritto, giustizia e logiche del dominio*, 2007, pp. 1000-1062.

del potere. La tecnologia, in questo senso, non è un mero strumento neutro, ma un fattore di trasformazione della normatività stessa.

La distinzione classica tra controllo formale (esercitato tramite il diritto e le istituzioni) e controllo informale (opinione pubblica, stigma sociale, consuetudini) risulta oggi problematica[3].

I sistemi tecnologici di sorveglianza e profilazione operano infatti in una zona grigia, in cui elementi tipici dell'uno e dell'altro si sovrappongono. Infatti, il controllo tecnologico: non si esaurisce nella sanzione giuridica, non necessita sempre di una decisione individualizzata, agisce spesso prima della violazione in chiave preventiva o predittiva.

Si assiste così ad un passaggio paradigmatico: dal controllo *ex post*, fondato sull'accertamento di un illecito, a un controllo *ex ante,* basato sulla previsione statistica del comportamento[4].

Questo mutamento incide direttamente su categorie fondamentali del diritto moderno: responsabilità, imputabilità, colpevolezza.

La tecnologia non è esterna al potere, ma ne costituisce una modalità di esercizio. Come mostrato dalla riflessione foucaultiana, il potere moderno non si manifesta solo nella legge che proibisce, ma nelle tecniche che normalizzano[5].

I sistemi tecnologici di controllo sociale – algoritmi, mega dati, intelligenza artificiale – rappresentano una nuova forma di *governance*, fondata sulla gestione delle popolazioni attraverso i dati.

In tale contesto, il diritto rischia una duplice trasformazione: da limite al potere a infrastruttura del potere tecnologico, da strumento di garanzia a meccanismo di legittimazione *ex post*.

Il problema giuridico centrale non è dunque solo se esistano norme, ma quale funzione esse svolgano nel rapporto tra individuo e autorità.

[3] Sulla distinzione tra controllo formale e informale e sulla sua progressiva erosione, cfr. A. Antonilli, *Distorsioni sociali nelle comunità contemporanee*, 2024, pp. 11-62.

[4] Sul passaggio dal controllo repressivo al controllo preventivo e predittivo, v. L. Ferrajoli, *Giustizia e Politica: crisi e rifondazione del garantismo penale*, Laterza, 2024; più recentemente, M. Schuilenburg, *The security society: on power, surveillance and punishments. The pre-crime society*, Bristol University Press, 2021, pp. 43-62.

[5] M. Foucault, *Sorvegliare e punire*, trad. it., Einaudi, 1976, p. 195 ss.; Id., *Sicurezza, territorio, popolazione*, Feltrinelli, 2005, lezioni 1977-1978, sul concetto di governamentalità.

Uno degli snodi più critici è rappresentato dall'automazione decisionale. Quando decisioni che incidono su diritti, libertà o *status* giuridici sono affidate (in tutto o in parte) a sistemi algoritmici, emergono tensioni profonde con i principi classici dello Stato di diritto[6].

In particolare, il principio di legalità è messo in crisi dall'opacità degli algoritmi, il principio di prevedibilità è compromesso dalla dinamicità dei modelli, il diritto di difesa risulta svuotato se la decisione non è intellegibile.

Il rischio non è solo tecnico, ma costituzionale: il passaggio da un diritto conoscibile a un diritto "calcolato" segna una rottura epistemologica rispetto alla tradizione giuridica moderna[7].

Come osservato dalla dottrina internazionale sui diritti umani[8], la prevedibilità della norma costituisce un elemento strutturale del principio di legalità, non solo in senso formale, ma sostanziale. In questo senso, la progressiva opacizzazione delle decisioni pubbliche mediante algoritmi mette in crisi quella *qualità della legge* che il diritto internazionale richiede quale condizione di legittimità delle interferenze statali nei diritti fondamentali.

In questo quadro, i diritti fondamentali non possono essere considerati una variabile accessoria. Essi costituiscono la bussola teorica per valutare la legittimità dei sistemi di controllo tecnologico.

Riservatezza, dignità, uguaglianza, libertà personale non sono meri interessi bilanciabili, ma limiti strutturali al potere[9].

Dal punto di vista della teoria generale del diritto, ciò implica una scelta di fondo: o il diritto accompagna la tecnologia, adattandosi alle

[6] Sul rapporto tra automazione decisionale e Stato di diritto, cfr. F. Pasquale, *The Black Box Society. The secret algorithms that control money*, Harvard University Press, 2015.

[7] Sul concetto di "crisi epistemologica" del diritto nell'era algoritmica, v. G. Teubner, *Law as an Autopoietic System*, Blackwell, 1993; M. Hilderbrandt, *Smart Technologies and the End(s) of Law. Novel entanglements of law and technology*, Edward Elgar, 2015.

[8] G.G. Fitzmaurice, *The general principles of international law, considered from the standpoint of the rule of law*, in *Recueil des cours de l'Académie de La Haye*, vol. 92, 1957-II, p. 7. Per approfondimenti, v. A. Cassese, *I diritti umani nel mondo contemporaneo*, Laterza, 2004.

[9] Sulla funzione dei diritti fondamentali come limiti strutturali al potere, cfr. G. Zagrebelsky, *Il diritto mite*, Einaudi, 1992; R. Alexy, *Teoria dei diritti fondamentali*, trad. it., Il Mulino, 2012.

sue logiche oppure il diritto riafferma la propria funzione critica, ponendo vincoli sostanziali e procedurali.

Il caso cinese, che verrà analizzato nei paragrafi successivi, rappresenta un laboratorio giuridico paradigmatico: un ordinamento che utilizza il diritto per organizzare il controllo tecnologico, ma che mostra al contempo le fragilità di una tutela dei diritti subordinata alla sicurezza e alla stabilità sociale[10].

La tecnologia non incide sul diritto solo come oggetto di regolazione, ma come fattore strutturale di trasformazione della normatività stessa[11].

Questa affermazione segna un punto di rottura rispetto alla concezione classica della norma giuridica, intesa come comando generale e astratto, posto da un'autorità legittimata e applicato *ex post* mediante un procedimento formalizzato.

Nel contesto delle tecnologie digitali, ed in particolare dei sistemi algoritmici di controllo sociale, la normatività tende a trasmigrare: dalla regola testuale alla procedura tecnica, dalla prescrizione esplicita alla configurazione dell'ambiente, dalla sanzione giuridica all'incentivo o disincentivo sistemico[12].

Si afferma così una forma di normatività immanente, che non si presenta come norma, ma che orienta efficacemente i comportamenti.

La teoria generale del diritto ha tradizionalmente individuato nella forma il tratto distintivo della normatività giuridica: generalità, astrattezza, pubblicità, prevedibilità[13].

[10] In chiave comparata e critica rispetto ai modelli autoritari tecnologicamente avanzati, v. S. Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019, spec. cap. 12; S. Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law*, Cambridge University Press, 2021.

[11] Sull'idea che la tecnologia incida sulla struttura della normatività e non solo sui suoi oggetti, v. I. Van De Poel, *Introduction: Technology and Normativity*, in *Techné: Research in Philosophy and Technology*, 2006, 10.1, pp. 1-6.

[12] Cfr. L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, 1999, p. 89 ss.; J. Reidenberg, *Lex Informatica. The formulation of information policy rules through technology*, in *Texas Law Review*, 1997, p. 553 ss.

[13] Per la concezione classica della norma giuridica come comando generale e astratto, v. H. Kelsen, *Teoria pura del diritto*, trad. it., Einaudi, 1966, p. 30 ss.; N. Bobbio, *Teoria generale del diritto*, Einaudi, 1993.

I sistemi tecnologici mettono in discussione ciascuno di questi elementi. L'algoritmo non è generale, ma profilato, non è astratto, ma contestuale, non è stabile, ma dinamico, non è, di regola, pubblico, ma (spesso) opaco[14].

Il risultato è una normatività che opera senza dichiararsi come tale, ma che produce effetti giuridicamente rilevanti: esclusioni, limitazioni, priorità, classificazioni.

Si tratta di una funzionalizzazione del diritto, in cui la conformità comportamentale è ottenuta non attraverso l'obbedienza alla norma, ma tramite l'adeguamento al sistema.

Un tratto decisivo del mutamento in atto è l'anticipazione normativa. La normatività tecnologica non interviene a valle di una violazione, ma a monte del comportamento, orientandolo in base a previsioni probabilistiche[15].

Ciò comporta uno slittamento concettuale rilevante: dalla responsabilità per fatti a una responsabilità per rischio; dall'imputazione individuale alla valutazione statistica; dalla colpevolezza alla pericolosità presunta.

Dal punto di vista dei diritti fondamentali, questo modello entra in tensione con: la presunzione di innocenza; il principio di personalità della responsabilità; il diritto a non essere sottoposti a decisioni arbitrarie[16].

In tale inedito contesto, il diritto corre il rischio di mutare funzione: da limite al potere a infrastruttura del potere tecnologico[17].

Le norme non operano più principalmente per contenere l'uso della tecnologia, ma per: abilitarne l'implementazione; organizzarne la cooperazione tra attori pubblici e privati; legittimarne gli effetti in nome di interessi superiori (sicurezza, ordine, efficienza).

[14] Cfr. F. Pasquale, *The Black Box Society*, Harvard University Press, 2015, p. 3 ss.; S. Lu, *Data privacy, human rights, and algorithmic opacity*, in *California Law Review*, 2022, 110, p. 2087 ss.

[15] B. Harcourt, *Against Prediction*, University of Chicago Press, 2006; D. Lyon, *Surveillance Society*, Open University Press, 2001.

[16] C. Sherman, *Confronting Algorithms: Conscience Catching in the Criminal Trial and Beyond*, in *University of Michigan Journal of Law Reform*, 2023, 57, p. 787 ss.

[17] L. Torchia, *Poteri pubblici e poteri privati nel mondo digitale*, il Mulino, 2024, 73.1, pp. 14-33; G. Agamben, *Stato di eccezione*, Bollati Boringhieri, 2003.

Il diritto diventa così condizione di possibilità del controllo, anziché strumento di garanzia. Questo slittamento è particolarmente evidente negli ordinamenti che privilegiano una concezione strumentale dei diritti, subordinandoli a fini collettivi definiti dall'autorità.

Il mutamento della normatività non è un fenomeno neutro. Esso incide direttamente sulla struttura dei diritti fondamentali, che rischiano di essere: frammentati, relativizzati, resi dipendenti da valutazioni algoritmiche non sindacabili[18].

Se i diritti fondamentali costituiscono, nella tradizione giuridica occidentale, limiti invalicabili al potere[19], la normatività tecnologica tende invece a trasformarli in variabili di sistema, bilanciabili in funzione dell'efficienza o della sicurezza.

Il caso della Repubblica popolare cinese rappresenta un banco di prova esemplare. Qui il mutamento della normatività si manifesta in forma esplicita e istituzionalizzata: la tecnologia non è solo utilizzata dal potere, ma è integrata nel disegno normativo dello Stato[20]. Il diritto non limita strutturalmente il controllo tecnologico, ma lo organizza e lo giustifica in nome della stabilità sociale e della sicurezza nazionale.

Nei capitoli successivi si analizzerà come questo mutamento della normatività si rifletta: nell'architettura concreta dei sistemi di controllo; nella legislazione su sicurezza, dati e informazione personale; nella configurazione (e nei limiti) della tutela dei diritti fondamentali.

2. L'architettura del controllo tecnologico nel fu Celeste Impero, l'odierna Repubblica popolare cinese, si fonda su un presupposto strutturale: la piena integrazione tra infrastrutture digitali e apparato statale[21].

[18] M. Miao, *Rule by algorithm*, *Columbia Journal of Transnational Law*, 2025, 63, p. 690.

[19] C. Focarelli, *Diritto internazioanle*, Cedam, 2021, pp. 502 ss; B. Conforti, *Diritto internazionale*, Editoriale Scientifica, 2021, pp. 222 ss.

[20] R. Suttmeier - Y. Xiangkui- A. Zixiang Tan, *Standards of power? Technology, institutions, and politics in the development of China's national standards strategy*, in *Geopolitics, History, and International Relations*, 2009, 1.1, pp. 46-84.

[21] M. Bicchiri, *Asia e intelligenza artificiale. Strategie, regolamentazione e sfide globali*, in *La Nuova Giurisprudenza Civile Commentata*, 2025, 3, p. 798.

A differenza di quanto avviene in molti ordinamenti occidentali, in cui le tecnologie digitali sono sviluppate prevalentemente dal mercato e successivamente regolamentate dal diritto, nel modello cinese esse sono concepite fin dall'origine come strumenti di governo[22].

Il controllo tecnologico non opera dunque ai margini dello Stato, ma nel suo cuore funzionale, divenendo parte integrante delle politiche pubbliche di sicurezza, ordine e amministrazione; in tutto ciò la gestione dei mega dati rappresenta il pilastro del sistema.

Infatti, attraverso la raccolta e l'aggregazione di una quantità massiva di informazioni – dati biometrici, transazioni economiche, spostamenti, comunicazioni digitali – lo Stato costruisce una visione integrata della popolazione, orientata non alla tutela del singolo, ma alla gestione preventiva del rischio.

L'intelligenza artificiale consente di trasformare i dati in strumenti decisionali, mediante: analisi predittive; classificazioni comportamentali; valutazioni di affidabilità o pericolosità.

Dal punto di vista giuridico, ciò comporta uno spostamento rilevante: dall'intervento fondato su un illecito accertato all'intervento fondato su modelli statistici.

La pubblica sicurezza diventa così il luogo privilegiato di sperimentazione di una normatività algoritmica, nella quale la decisione non è il risultato di una valutazione giuridica individualizzata, ma di una elaborazione probabilistica[23].

Un ruolo centrale è, poi, svolto dai sistemi di videosorveglianza intelligente, integrati con tecnologie di riconoscimento facciale e analisi comportamentale. Questi strumenti consentono non solo di identificare gli individui, ma di tracciarne gli spostamenti, associare immagini a profili digitali, correlare comportamenti a valutazioni di rischio[24].

[22] Y. Chen, *China's digital economy development: Incentives and challenges*, in *Technological and Economic Development of Economy*, 2023, 29.2, pp. 518-538.

[23] R. Peeters, *Machine justice: Governing security through the bureaucracy of algorithms*, in *Information Polity*, 2018, 23.3, pp. 267-280.

[24] X. Qiang, *The road to digital unfreedom: President Xi's surveillance state*, in *Journal of Democracy*, 2019, 30.1, pp. 53-67; L. Liang Pinghan - G. Yuchen, *Local Governments and the Diffusion of Video Surveillance in China: Evidence from the Public Procurement Contracts*, in *Journal of Chinese Political Science*, 2025, pp. 1-27.

La polizia predittiva rappresenta il punto di convergenza di tali tecnologie. Essa non si limita a supportare l'attività investigativa, ma orienta decisioni preventive, quali: intensificazione della sorveglianza; controlli mirati; restrizioni indirette.

Dal punto di vista dei diritti fondamentali, il problema non risiede solo nella sorveglianza in sé, ma nella normalizzazione del controllo permanente, che incide: sulla libertà di movimento; sull'anonimato nello spazio pubblico; sulla dignità della persona.

La logica predittiva entra in tensione con principi cardine dello Stato di diritto, quali la presunzione di innocenza e la necessità di una base fattuale individuale per l'intervento pubblico[25].

3. Il Sistema di Credito Sociale[26] costituisce uno degli elementi più discussi dell'architettura del controllo tecnologico cinese. Tuttavia, una sua analisi giuridicamente rigorosa impone di superare letture semplificatrici o meramente mediatiche. Il sistema non è un'unica base dati centrale, ma un insieme eterogeneo di programmi, sviluppati a livello nazionale e locale, che condividono una medesima razionalità di fondo: valutare e orientare il comportamento dei consociati attraverso strumenti reputazionali e tecnologici[27].

Le origini del Sistema di Credito Sociale sono rintracciabili in documenti programmatici del Consiglio di Stato, in particolare nel *Planning Outline for the Construction of a Social Credit System* (2014–2020)[28].

Il lessico utilizzato è rivelatore: il sistema è finalizzato a costruire una "società della fiducia" (*trustworthy society*), nella quale l'affidabilità diventa una categoria cardine dell'ordine sociale. Tale affidabilità non è, però, concepita come virtù etica privata, bensì come qualità misurabile e verificabile, suscettibile di valutazione pubblica.

[25] M. Dorf, *Prediction and the Rule of Law*, in *UCLA Law Review*, 1994, 42, p. 651.

[26] Y. Laniuk, *Social credit system as a panopticon: Surveillance and power in the digital age*, in *Community and tradition in global times*, 2021, pp. 211-234.

[27] F. Liang - C. Yuchen, *The making of "good" citizens: China's Social Credit Systems and infrastructures of social quantification*, in *Policy & Internet*, 2022, 14.1, pp. 114-135.

[28] *Planning Outline for the Construction of a Social Credit System (2014–2020)*, State Council of the People's Republic of China, 14 giugno 2014.

Tali documenti evidenziano una finalità esplicita: rafforzare la fiducia sociale e l'ordine economico mediante meccanismi di valutazione dell'affidabilità.

Sul piano giuridico, colpisce il fatto che il sistema nasca prima e al di fuori di una legge quadro, sviluppandosi attraverso: regolamenti amministrativi, progetti pilota, cooperazione pubblico-privato.

Ebbene, il controllo reputazionale precede la sua formalizzazione normativa, confermando il ruolo della tecnologia come fattore primario di normatività.

Il Sistema di Credito Sociale svolge una duplice funzione.

La prima è una funzione disciplinare[29], attraverso meccanismi di premio e punizione: accesso o esclusione da servizi; facilitazioni o restrizioni economiche; limitazioni indirette della mobilità o delle opportunità. Le conseguenze di una valutazione negativa non assumono, di regola, la forma di una sanzione penale o amministrativa tipizzata, bensì di restrizioni nell'accesso a servizi pubblici o privati, limitazioni alla mobilità, esclusioni da opportunità economiche o professionali. Si tratta di sanzioni indirette, spesso cumulative, che incidono in modo significativo sulla vita dell'individuo senza attivare le garanzie proprie del procedimento giuridico[30].

Il problema è duplice: l'assenza di una base legale chiara e prevedibile e la difficoltà di individuare un atto impugnabile. Il controllo disciplinare opera così in una zona grigia, sottratta ai tradizionali meccanismi di tutela. Tale zona può essere letta, sul piano teorico, come un'area di normatività materiale priva di formalizzazione legislativa, ma produttiva di effetti giuridicamente rilevanti. La dottrina internazionalistica ha evidenziato come i diritti umani possano essere compressi non solo mediante atti normativi formali, ma anche attraverso pratiche amministrative sistemiche e dispositivi tecnici, che aggirano i presupposti di legalità, prevedibilità e controllabilità giurisdizionale[31].

[29] L. Orgad - W. Rejers, *A dystopian future? The rise of social credit systems* in *The Rise of Social Credit Systems*, *Robert Schuman Centre for Advanced Studies* Research, 94, 2019.

[30] M. Von Blomberg, *The social credit system and China's rule of law. Social Credit Rating: Reputation und Vertrauen beurteilen*, Wiesbaden, Springer, 2020, pp. 111-137.

[31] M. Hilderbrandt, *Smart technologies and the end(s) of law*, Cheltenham, 2015, p. 85 ss; L. Ferrajoli, *Principia Iuris. Teoria del diritto e della democrazia*, vol. I, Roma-Bari, 2007, p. 807.

La seconda è una funzione reputazionale, che incide sullo *status* sociale dell'individuo. La reputazione diventa una categoria quasi-giuridica, capace di produrre effetti concreti senza il ricorso a una sanzione formale[32]. Il comportamento conforme, pertanto, non è richiesto dalla legge, ma indotto dal sistema.

Ciò implica una trasformazione profonda: la dignità personale viene indirettamente condizionata da indicatori quantitativi; lo *status* sociale è mediato da sistemi di *scoring*; la conformità comportamentale è incentivata tramite visibilità pubblica o stigmatizzazione.

Nell'ottica dei diritti fondamentali, questo modello solleva interrogativi profondi: assenza di un procedimento garantito; difficoltà di contestazione; confusione tra valutazione morale e valutazione giuridica.

Uno degli aspetti più problematici del Sistema di Credito Sociale è la mancanza di un quadro normativo unitario e sistematico.

Non esiste una legge generale che definisca chiaramente i criteri di valutazione, stabilisca diritti procedurali uniformi e garantisca rimedi effettivi. Il Sistema si configura piuttosto come una rete policentrica di sistemi locali, *blacklist* e *redlist*; programmi settoriali (finanziari, amministrativi, giudiziari); piattaforme gestite in cooperazione con attori privati[33].

Questa frammentazione normativa produce una zona di indeterminatezza giuridica, in cui il controllo tecnologico opera con ampia discrezionalità amministrativa. Epperò, tale frammentazione non è un difetto contingente, ma una scelta funzionale perché consente sperimentazione continua, riduce la necessità di una base legislativa rigida, amplia la discrezionalità amministrativa.

Dal punto di vista della teoria delle fonti, il controllo sociale viene così esercitato al di sotto ed ai margini della legge, attraverso strumenti che producono effetti sostanzialmente normativi senza assumere forma legislativa.

[32] C. Loefflad - M. Chen - J. Grosskglas, *Reputational discrimination and fairness in China's social credit system*, in *Digital Government: Research and Practice*, 2024, 5.4, pp. 1-27.

[33] Z. Zuo, *Governance by algorithm: China's Social credit system*, University of Cambridge, 2020.

Ciò conferma che il Sistema di Credito Sociale non è solo uno strumento di politiche pubbliche, ma una forma di normatività tecnologica decentrata, che incide sui diritti senza assumere la forma della legge.

4.1. La *Cybersecurity Law* della Repubblica popolare cinese, entrata in vigore il 1° giugno 2017, costituisce il perno normativo originario della governance digitale cinese.

Essa si presenta formalmente come una legge di equilibrio tra sicurezza, sviluppo tecnologico e tutela dei diritti, ma nella sua struttura sostanziale rivela una netta prevalenza della sicurezza statale[34].

All'art. 1 si individuano finalità e struttura della legge: «La presente legge è formulata allo scopo di garantire la sicurezza informatica, salvaguardare la sovranità cibernetica nazionale, la sicurezza e gli interessi dello Stato, nonché i diritti e gli interessi legittimi dei cittadini, delle persone giuridiche e delle altre organizzazioni». La disposizione è paradigmatica: i diritti individuali sono menzionati, ma in posizione subordinata rispetto alla sicurezza e alla sovranità. Dal punto di vista della teoria dei diritti fondamentali, si tratta di una tutela strumentale, non assiologica.

Circa gli obblighi di cooperazione e controllo statale, l'art. 28 recita: «Gli operatori di rete devono fornire supporto tecnico e assistenza alle autorità di pubblica sicurezza e agli organi di sicurezza dello Stato per la tutela della sicurezza nazionale e l'investigazione di reati». La norma impone un obbligo generalizzato di collaborazione, privo di limiti sostanziali, garanzie procedurali, controllo giurisdizionale espresso. Ciò incide direttamente su libertà di impresa, riservatezza delle comunicazioni, protezione dei dati personali.

Altro esempio normativo critico lo si ha in tema di localizzazione dei dati e sovranità digitale all'art. 37 che dichiara: «I dati personali e i dati importanti raccolti e prodotti dagli operatori di infrastrutture critiche devono essere conservati all'interno del territorio della Repubblica popolare cinese». Questa disposizione rafforza la sovranità statale sui dati, ma al contempo facilita l'accesso delle autorità, riduce le garanzie contro interferenze arbitrarie, limita la tutela transnazionale dei diritti.

[34] R. Creemers, *Cybersecurity law and regulation in China: Securing the smart state*, in *China Law and Society Review*, 2023, 6.2, pp. 111-145.

Si individuano, dal tenore della legge, delle criticità sistemiche: essa non riconosce un diritto autonomo alla iservatezza, utilizza concetti giuridici indeterminati ("sicurezza", "interessi dello Stato"), attribuisce ampi poteri discrezionali all'amministrazione. Dunque, opera come infrastruttura normativa del controllo tecnologico, più che come strumento di garanzia[35].

4.2. La *National Intelligence Law*, adottata nel giugno 2017, rappresenta una delle norme più problematiche dal punto di vista dei diritti fondamentali, poiché estende il paradigma della sicurezza all'intera società[36].

All'art. 7 si prevede un obbligo generalizzato di cooperazione: «Ogni organizzazione e cittadino deve sostenere, assistere e cooperare con il lavoro di intelligence nazionale in conformità alla legge». La norma non distingue tra cittadini, imprese, professionisti, non prevede eccezioni fondate su diritti fondamentali, non stabilisce limiti sostanziali o procedurali. Dal punto di vista dello Stato di diritto, si tratta di un obbligo di lealtà assoluta, incompatibile con una concezione forte della libertà individuale.

All'art. 10 si definiscono i poteri degli organi di *intelligence*: «Gli organi di intelligence nazionale possono adottare le misure necessarie per svolgere il lavoro di intelligence». L'uso dell'espressione "misure necessarie" introduce una clausola di onnipotenza funzionale, priva di tipizzazione, proporzionalità espressa, controllo giurisdizionale effettivo.

In sintesi, tale normativa incide in modo diretto su libertà personale, libertà di espressione, diritto alla riservatezza, segretezza delle comunicazioni. Il cittadino non è titolare di diritti opponibili allo Stato, ma risorsa funzionale alla sicurezza nazionale[37].

[35] A. Qi - S. Shao - W. Zheng, *Assessing China's cybersecurity law*, in *Computer law & security review*, 2018, 34.6, pp. 1342-1354.

[36] C. Jing, *The Impact of National Security on Human Rights: A Comparative Study of Practice under the ECHR and in China*, Utrecht University, 2023.

[37] D. Han, *On the Relations between National Security and Human Rights Defined in the Constitution of the People's Republic of China*, in *Journal of Human Rights*, 2019, 18, p. 551.

4.3. La Data Security Law, entrata in vigore nel 2021, consolida la visione dei dati come risorsa strategica nazionale[38].

All'art. 21, sulla classificazione dei dati, si afferma che lo Stato istituisce un sistema di classificazione e protezione dei dati basato sull'importanza dei dati per lo sviluppo economico e sociale e per la sicurezza nazionale. La tutela dei dati è così subordinata alla loro rilevanza sistemica, non alla posizione giuridica dell'individuo.

All'art. 45, sul primato della sicurezza nazionale, si dichara che qualsiasi organizzazione o individuo che svolga attività di trattamento dei dati deve rispettare le leggi e i regolamenti e adempiere agli obblighi di sicurezza dei dati. Il riferimento ai diritti individuali è assente. Il dato non è tutelato come proiezione della persona, ma come bene strategico dello Stato.

La legge, pertanto, non riconosce un diritto soggettivo alla protezione dei dati, rafforza la discrezionalità amministrativa, consolida la subordinazione dell'individuo alla sicurezza collettiva.

4.4. La *Personal Information Protection Law* (PIPL) è spesso presentata come il tentativo cinese di avvicinarsi ai modelli occidentali di tutela dei dati personali. Tuttavia, tale convergenza è solo apparente[39].

All'art. 4 si trova la definizione di informazione personale: «Le informazioni personali sono tutte le informazioni, registrate elettronicamente o in altro modo, relative a una persona fisica identificata o identificabile». La definizione è ampia e in linea con gli *standards* internazionali.

All'art. 13, le basi legali del trattamento: «Il trattamento delle informazioni personali è consentito quando necessario per l'adempimento di responsabilità legali o obblighi statutari». La clausola consente un amplissimo margine di intervento statale, senza un reale bilanciamento.

Al Capitolo 2, Sezione 3, artt. 33-37, vi sono le eccezioni per lo Stato secondo cui il trattamento di informazioni personali da parte degli organi statali per l'adempimento delle loro funzioni è disciplinato dalla

[38] J. Chen - J. Sun, *Understanding the chinese data security law*, in *International Cybersecurity Law Review*, 2021, 2.2 pp. 209-221.

[39] R. Ong, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, 2023, 31.4, pp. 349-375.

presente legge e da altre leggi pertinenti. Il rinvio ad "altre leggi" – in particolare a quelle sulla sicurezza – svuota la tutela, subordinandola a esigenze superiori. La PIPL, dunque, riconosce diritti formali (accesso, rettifica), ma non prevede un'autorità indipendente, né strumenti effettivi di opposizione allo Stato. I diritti sono concessi, non opponibili[40].

5. L'analisi delle principali leggi tecnologiche della Repubblica Popolare Cinese mette in luce una costante strutturale: la presenza esplicita di un linguaggio dei diritti, accompagnata tuttavia da una sistematica neutralizzazione della loro funzione garantista. La tutela dei diritti fondamentali viene evocata sul piano dichiarativo, ma non assunta come criterio di validità e limite del potere pubblico.

Nella *Cybersecurity Law*, nella *Data Security Law* e nella *Personal Information Protection Law*, i diritti compaiono prevalentemente nei considerando iniziali, come obiettivi accessori (anche nella loro collocazione sistematica, spesso al termine delle singole disposizioni) o come interessi da proteggere "insieme" alla sicurezza nazionale. Questa tecnica normativa realizza una forma di retorica giuridica dei diritti: il lessico della protezione è impiegato per legittimare l'espansione del potere statale, non per contenerlo.

Avendo sempre come bussola la teoria dei diritti fondamentali, ciò equivale a un rovesciamento della loro funzione: i diritti non operano più come controlimiti, ma come argomenti di giustificazione dell'intervento pubblico. Emblematico è, poi, il ricorso a formule indeterminate quali: "sicurezza nazionale", "interessi fondamentali dello Stato", "ordine sociale" che assorbono e subordinano ogni posizione soggettiva. Il bilanciamento non avviene tra diritti e poteri, ma all'interno del potere stesso, secondo una logica autoriferita.

In questa prospettiva, la legge non è strumento di garanzia, ma meccanismo di razionalizzazione del controllo.

Il diritto positivo assume una funzione performativa, dichiarando di tutelare i diritti, contribuisce a rendere accettabile la loro compressione. Dal punto di vista assiologico, si è in presenza non di un ordi-

[40] J. Yang, *An Overview of the Chinese Personal Information Protection Law*, in *Pin Code*, 2022, 10.1, pp. 8-13.

namento dei diritti, ma di un ordinamento della sicurezza, nel quale la persona non è fine, bensì oggetto regolato. La distanza rispetto al costituzionalismo dei diritti è quindi strutturale, non contingente.

Se la legge costituisce il veicolo formale del controllo, la tecnologia ne rappresenta il moltiplicatore materiale.

Nel contesto cinese, l'innovazione tecnologica non si limita a potenziare l'efficacia dell'azione amministrativa, ma trasforma qualitativamente l'esercizio del potere. *Big data*, intelligenza artificiale, videosorveglianza e sistemi predittivi producono una mutazione profonda della normatività: il controllo non è più episodico o reattivo, ma continuo, preventivo e pervasivo[41].

Dal punto di vista giuridico, ciò comporta almeno tre conseguenze fondamentali, vale a dire l'anticipazione della soglia di intervento (il potere pubblico agisce prima della violazione, sulla base di probabilità e correlazioni statistiche); la depersonalizzazione della decisione (il soggetto non è valutato per ciò che ha fatto, ma per ciò che il sistema prevede possa fare); opacità del potere (l'algoritmo sostituisce la motivazione giuridica, rendendo il controllo difficilmente contestabile)[42].

In questo scenario, la tecnologia diviene una fonte materiale di normatività, capace di incidere sui comportamenti senza passare attraverso la forma classica della legge. Il potere non ordina, ma configura ambienti, incentivi, reputazioni. La conseguenza più rilevante, sul piano dei diritti fondamentali, è l'erosione della libertà come spazio di autodeterminazione.

Il soggetto interiorizza il controllo, adattando il proprio comportamento a criteri che non conosce e non può contestare. Siamo così oltre il paradigma foucaultiano della sorveglianza: la tecnologia non osserva soltanto, ma produce conformità.

Nel sistema cinese, questo processo è ulteriormente rafforzato dall'assenza di un giudice indipendente, un'autorità di controllo autonoma, una sfera inviolabile dei diritti.

[41] X. Wu, *Technology, power, and uncontrolled great power strategic competition between China and the United States*, in *China International Strategy Review*, 2020, 2.1, pp. 99-119.

[42] P. Liang - X. Li - Y. Guo, *Local Governments and the Diffusion of Video Surveillance in China: Evidence from the Public Procurement Contracts*, *Journal of Chinese Political Science*, 2025, pp. 1-27.

Il risultato è un potere statale potenziato, nel quale diritto e tecnologia convergono non per limitarsi reciprocamente, ma per potenziarsi[43].

6. L'analisi del modello cinese sul controllo tecnologico acquista piena rilevanza giuridica solo se collocata entro il quadro normativo del diritto internazionale ed europeo dei diritti umani, che individua obblighi giuridici vincolanti per gli Stati in materia di sorveglianza, trattamento dei dati e automazione decisionale. In tale prospettiva, la questione non è se la tecnologia sia regolata, bensì se e in che misura l'uso del controllo tecnologico sia compatibile con i principali parametri internazionali di tutela dei diritti fondamentali.

A livello universale, il diritto alla vita privata è consacrato all'art. 12 della Dichiarazione universale dei diritti dell'uomo del 1948 (seppur non giuridicamente vincolante in quanto risoluzione ONU) e, soprattutto, all'art. 17 del Patto internazionale sui diritti civili e politici (o ICCPR, 1966), secondo cui: «Nessuno può essere sottoposto a interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza».

Giova sottolineare che, per quanto concerne la Repubblica popolare cinese, l'anzidetto Patto non è, ad oggi, ancora stato ratificato, bensì solo firmato dal proprio ambasciatore il 5 ottobre 1998, con le preoccupanti conseguenze del caso (si rammenta, invece, che la Repubblica di Cina guidata dai nazionalisti di Chiang Kai-shek, prima dell'avvento dell'attuale regime, ricoprì un ruolo di primo piano nella stesura della Dichiarazione suddetta).

La norma è, comunque, di particolare rilievo perché ormai espressione di quei principi generali di diritto riconosciuti dalle nazioni civili menzionati nell'art. 38 dello Statuto della Corte Internazionale di Giustizia, ciò in quanto non solo vieta non le interferenze illegali, ma anche quelle arbitrarie, introducendo un limite sostanziale all'azione statale. Come chiarito dal Comitato per i diritti umani delle Nazioni Unite (General Comment n. 16/1988)[44], un'interferenza è arbitraria quando,

[43] G. Abiri - X. Huang, *The People's (Republic) Algorithms*, in *Notre Dame Journal of International and Comparative Law*, 2022, 12, p. 16.

[44] Comitato per i diritti umani, General Comment no. 16: Article 17 (*Right to Privacy*), 8 aprile 1988, HRI/GEN/1/Rev. 9.

pur prevista dalla legge, non rispetta i criteri di ragionevolezza, necessità e proporzionalità.

La dottrina ha sottolineato come il divieto di interferenze arbitrarie configuri un limite sostanziale al potere statale, che non può essere aggirato mediante la mera formalizzazione legislativa dell'ingerenza. In questa prospettiva, l'arbitrarietà non coincide con l'illegalità, ma con la mancanza di proporzionalità, necessità e controllo indipendente dell'interferenza[45].

I sistemi di sorveglianza tecnologica permanente, di raccolta massiva di dati e di profilazione predittiva – quali quelli analizzati nel caso cinese – pongono dunque un problema di compatibilità con l'art. 17 ICCPR nella misura in cui operano in modo generalizzato e indiscriminato, non richiedono una base fattuale individualizzata, non sono sottoposti a un controllo indipendente effettivo.

A ciò si aggiunge l'art. 2, par. 3, ICCPR, che impone agli Stati l'obbligo di garantire un ricorso effettivo contro le violazioni dei diritti riconosciuti dal Patto, requisito che in Cina, come visto nei precedenti paragrafi, risulta strutturalmente compromesso in assenza di un giudice indipendente e di rimedi giurisdizionali effettivi.

Nel sistema del Consiglio d'Europa, l'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU) tutela il diritto al rispetto della vita privata e familiare. Ogni ingerenza dell'autorità pubblica è ammessa solo se prevista dalla legge, diretta a uno scopo legittimo (sicurezza nazionale, ordine pubblico, prevenzione dei reati), necessaria in una società democratica.

La giurisprudenza consolidata della Corte EDU ha precisato che il requisito della "legge" implica non solo una base normativa formale, ma anche accessibilità, prevedibilità e precisione della disciplina (sentenze Sunday Times c. Regno Unito del 26 aprile 1979 in relazione alla violazione dell'art. 10 CEDU, Zakharov c. Russia del 4 dicembre 2015 in relazione alla violazione dell'art. 8 CEDU, Big Brother Watch c. Regno Unito del 25 maggio 2021 in relazione alla violazione degli artt. 8 e 10 CEDU)[46].

[45] U. Pagallo, *Il diritto nell'età dellinformazione*, Giappichelli, 2014, p. 166 ss.

[46] CtEDU, Sunday Times c. Regno Unito (n. 1), sentenza 26 aprile 1979, ric. n. 6538/74, § 49, in cui la Corte chiarisce che la nozione di "legge" ai sensi dell'art. 10 (e, per estensione, dell'art. 8) CEDU richiede che la norma sia accessibile al cittadino e formulata

In materia di sorveglianza tecnologica, la Corte ha inoltre richiesto limiti chiari all'estensione e alla durata della sorveglianza, criteri rigorosi per l'accesso ai dati, controllo preventivo o successivo da parte di un'autorità indipendente, possibilità di ricorso giurisdizionale.

Alla luce di tali parametri, un sistema di controllo tecnologico fondato su clausole ampie di sicurezza nazionale, privo di limiti sostanziali e sottratto a un controllo giurisdizionale indipendente, risulta difficilmente conciliabile con l'art. 8 CEDU.

Nell'ordinamento dell'Unione europea, la tutela è ulteriormente rafforzata dall'art. 7 (vita privata) e dall'art. 8 (protezione dei dati personali) della Carta dei diritti fondamentali dell'UE. Quest'ultimo riconosce espressamente che i dati devono essere trattati per finalità determinate, sulla base del consenso o di un'altra base legittima prevista dalla legge e sotto il controllo di un'autorità indipendente.

Il Regolamento (UE) 2016/679 (RGPD) costituisce attuazione diretta di tali principi e introduce limiti stringenti al trattamento dei dati, tra cui: il principio di minimizzazione (art. 5); il principio di limitazione della finalità (art. 5); il diritto di opposizione (art. 21); il diritto a non essere sottoposti a decisioni basate unicamente su trattamenti automatizzati che producano effetti giuridici significativi (art. 22).

Quest'ultimo profilo è particolarmente rilevante nel confronto con i sistemi di scoring e valutazione reputazionale. L'art. 22 GDPR vieta tali decisioni salvo eccezioni rigorosamente tipizzate e comunque subordinate a garanzie adeguate, tra cui l'intervento umano e il diritto di contestazione.

con sufficiente precisione da consentire di prevedere, entro limiti ragionevoli, le conseguenze di una determinata condotta; CtEDU (Grande Camera), Roman Zakharov c. Russia, sentenza 4 dicembre 2015, ric. n. 47143/06, §§ 228-234, ove la Corte afferma che i sistemi di sorveglianza segreta devono essere accompagnati da garanzie adeguate e sufficienti contro gli abusi, tra cui limiti chiari all'ambito di applicazione, alla durata delle misure, alle modalità di accesso ai dati e un controllo indipendente effettivo, pena la violazione dell'art. 8 CEDU; CtEDU (Grande Camera), Big Brother Watch and Others c. Regno Unito, sentenza 25 maggio 2021, ricc. nn. 58170/13, 62322/14 e 24960/15, §§ 323-361, in cui la Corte ribadisce che i programmi di sorveglianza di massa sono compatibili con l'art. 8 CEDU solo se fondati su una base legale sufficientemente precisa e corredati da garanzie *end-to-end*, includendo un controllo indipendente, la supervisione continua e la possibilità di ricorso effettivo.

Nel modello cinese, invece, i sistemi di valutazione algoritmica producono effetti concreti sulla vita degli individui senza che siano previste garanzie procedurali equivalenti, né un diritto effettivo di opposizione allo Stato.

Il quadro europeo è ulteriormente completato dalla recente normativa sull'intelligenza artificiale (Regolamento UE 2024/1689 sull'IA)[47], che qualifica come ad alto rischio i sistemi di IA utilizzati per finalità di controllo sociale, valutazione del comportamento e accesso a diritti o servizi fondamentali[48].

In particolare, il regolamento vieta pratiche di social scoring da parte delle autorità pubbliche quando esse: producono trattamenti sfavorevoli sproporzionati; incidono su diritti fondamentali; si basano su comportamenti non direttamente rilevanti.

Questo divieto rende evidente la divergenza strutturale con il Sistema di Credito Sociale cinese, che utilizza lo *scoring* come strumento ordinario di governo della popolazione.

Nel diritto internazionale ed europeo dei diritti umani, i diritti fondamentali non si limitano a vietare interferenze arbitrarie, ma impongono obblighi positivi agli Stati: obbligo di prevenire abusi, di istituire garanzie procedurali, di assicurare rimedi effettivi.

Secondo la dottrina prevalente, gli obblighi positivi costituiscono oggi una componente strutturale della protezione internazionale dei diritti umani: lo Stato non è soltanto tenuto a non violare i diritti, ma anche a predisporre apparati normativi, procedurali e istituzionali idonei a prevenire abusi tecnologici e a garantire rimedi effettivi. L'assenza di autorità indipendenti di controllo e di meccanismi giurisdizionali effettivi integra pertanto una violazione strutturale degli *standards* internazionali[49].

Nel modello cinese, al contrario, il diritto opera prevalentemente come obbligo di cooperazione del cittadino con lo Stato (come previsto

[47] Regolamento UE 2024/1689, entrato in vigore nell'agosto 2024 e pienamente applicabile dal 2 agosto 2026.

[48] Artt. 5-6 ed Allegato III, Regolamento UE 2024/1689.

[49] A. Marchesi, *Diritti umani e Nazioni unite*, Franco Angeli, 2003, p. 102 ss.

dalla *National Intelligence Law*), ribaltando la logica del diritto internazionale, in cui è lo Stato a essere vincolato nei confronti dell'individuo.

Il confronto con le normative internazionali ed europee dimostra che la distanza tra il modello cinese e gli ordinamenti fondati sul diritto internazionale dei diritti umani non riguarda il grado di sviluppo tecnologico, bensì la struttura giuridica della limitazione del potere.

Là dove il diritto internazionale ed europeo costruisce la tecnologia come oggetto di vincoli giuridici stringenti, il modello cinese la integra come strumento ordinario di governo, sottraendola a un controllo giurisdizionale effettivo.

In questa prospettiva, il diritto internazionale dei diritti umani non fornisce solo criteri comparativi, ma costituisce il parametro normativo attraverso cui valutare quando il controllo tecnologico cessa di essere compatibile con un ordinamento fondato sulla centralità della persona.

Ebbene, da quanto surriportato, il confronto tra il modello cinese di *governance* tecnologica e i modelli occidentali non può essere risolto nei termini, troppo semplicistici, di una contrapposizione tra autoritarismo e democrazia[50]. La divergenza è più profonda e strutturale giacché riguarda il modo stesso di concepire il rapporto tra diritto, potere e individuo.

Nei modelli occidentali[51], pur tra contraddizioni e arretramenti, il costituzionalismo dei diritti continua a rappresentare il paradigma di legittimazione del potere. La tecnologia è considerata, almeno sul piano normativo, come oggetto di regolazione, e il diritto come strumento chiamato a porre limiti, garantire proporzionalità, assicurare giustiziabilità. La centralità dei diritti fondamentali – dalla protezione dei dati personali alla libertà di espressione – non è meramente retorica, ma si traduce in autorità indipendenti, controllo giurisdizionale, principio di legalità sostanziale.

[50] X. Hu - M. Li, *Ecopolitical discourse: Authoritarianism or democracy? Evidence from China*, in *PLoS One*, 2020, 15.10; B. Lin, *Beyond authoritarianism and liberal democracy: Understanding China's artificial intelligence impact in Africa* in *Information, Communication & Society*, 2024, 27.6, pp. 1126-1141.

[51] V. Pyrohovska, *Human rights protection in the context of information technology development: Problems and future prospects*, in *Futurity Economics&Law*, 2024, 4.1, pp. 38-51.

Nel modello cinese[52], al contrario, la tecnologia non è un fattore da contenere, ma una risorsa da integrare nell'esercizio del potere. Il diritto non opera come limite esterno, bensì come meccanismo interno di razionalizzazione e ottimizzazione del controllo.

La differenza decisiva non è quantitativa (più o meno sorveglianza), ma qualitativa: nei sistemi occidentali il potere deve giustificarsi davanti ai diritti; nel sistema cinese i diritti sono funzionalizzati alla stabilità del potere. Questo scarto riflette due diverse antropologie giuridiche: da un lato, l'individuo come titolare di diritti inviolabili; dall'altro, l'individuo come nodo di una rete sociale da governare.

Ne consegue che l'uso della tecnologia non produce gli stessi effetti giuridici: ciò che in Occidente è vissuto come eccezione da giustificare, in Cina è normalità da amministrare. Il rischio, tuttavia, non è unicamente esterno.

L'esperienza cinese funziona anche come specchio critico per l'Occidente, mostrando come, in assenza di un presidio forte dei diritti, la tecnologia possa progressivamente svuotare il costituzionalismo dall'interno, senza bisogno di rotture formali.

Se l'analisi comparata mette in luce la profondità delle divergenze, la riflessione teorica conclusiva impone una domanda radicale: è ancora possibile pensare i diritti fondamentali come limiti effettivi al potere tecnologico? Nel contesto cinese, la risposta – allo stato attuale – non può che essere negativa. I diritti sono riconosciuti formalmente, ma privati della loro funzione oppositiva. Essi non operano come barriere, bensì come variabili interne a un sistema orientato alla sicurezza e alla stabilità. Tuttavia, proprio questo dato consente di chiarire, per contrasto, la funzione autentica dei diritti fondamentali. Questi non sono semplici interessi protetti, né concessioni del legislatore, ma strutture di resistenza giuridica contro l'espansione del potere[53].

[52] O. Stovpets, *Digital technologies and human rights: challenges and opportunities*, in *Revista Amazonia Investiga*, 2023, 12.72, pp. 17-30.

[53] C. Padovani - M. Santaniello, *Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system*, in *International Communication Gazette*, 2018, 80.4, pp. 295-301.

In un'epoca in cui la tecnologia anticipa i comportamenti, rende invisibili le decisioni, dissolve la responsabilità, i diritti fondamentali rappresentano l'ultimo spazio di irriducibilità dell'umano al calcolo. Tuttavia, perché ciò avvenga, essi devono essere ripensati non solo come diritti "da proteggere", bensì come principi ordinatori del sistema tecnologico stesso. Non basta limitare l'uso degli algoritmi[54]: occorre costituzionalizzarli, assoggettandoli a trasparenza, controllabilità, responsabilità giuridica.

Il caso cinese dimostra cosa accade quando questa operazione non viene compiuta ovverossia che il potere tecnologico cresce senza attriti, il diritto perde la sua funzione critica e l'individuo si dissolve in una somma di dati. La posta in gioco non è solo giuridica, ma filosofica e politica poiché si tratta di decidere se la tecnologia debba servire la persona o se la persona debba adattarsi ai sistemi che la governano. In questa prospettiva, i diritti fondamentali non sono un residuo del passato, ma l'unico linguaggio giuridico ancora capace di dire "no" al potere, anche quando esso si presenta come neutro, efficiente e razionale[55].

Ed è proprio qui che il confronto con la Cina assume un valore paradigmatico: non come modello da imitare o respingere, ma come avvertimento sistemico su ciò che accade quando il diritto rinuncia alla sua vocazione limitativa[56].

[54] M. Sciacca, *Algocrazia e sistema democratico. Alla ricerca di una mite soluzione antropocentrica*, in *Contratt. e Impres.*, 2022, 4, p. 1173.

[55] E. Kosta, *Algorithmic state surveillance: Challenging the notion of agency in human rights*, in *Regulation & Governance*, 2022, 16.1, pp. 212-224.

[56] L. Han - P. De Stefani, *Protecting fundamental values through the global human rights sanction regime: China's challenges to the EU's normative power*, in *The International Journal of Human Rights*, 2025, 29.5, pp. 940-964.

LA PRIVACY NELL'ERA DELLO SPYWARE E DELLA SORVEGLIANZA DIGITALE

Pasquale Jari Borrata

1. Negli ultimi anni la rivoluzione digitale ha ridefinito profondamente le modalità di comunicazione, di lavoro e di accesso alle informazioni. Tuttavia, insieme ai benefici derivanti dall'innovazione tecnologica, si sono moltiplicate le preoccupazioni legate alla tutela della privacy e alla protezione dei diritti fondamentali. La crescente diffusione di strumenti di sorveglianza avanzati commercializzati da società private e destinati a governi e autorità statali, come gli spyware dalle società israeliane Paragon Solutions e NSO Group, ha reso ancora più urgente il dibattito su tali questioni.

Strumenti di sorveglianza di ultima generazione come Graphite, sviluppato da Paragon Solutions, e il più celebre Pegasus, creato dalla NSO Group, rappresentano esempi concreti di tecnologie capaci di minare la sfera privata degli individui. Questi software, che secondo quanto dichiarato dai produttori dovrebbero essere impiegati esclusivamente dai servizi di intelligence e dalle forze dell'ordine per il contrasto alla criminalità e al terrorismo[1], sono progettati per infiltrarsi nei dispositivi mobili e raccogliere dati senza il consenso né la consapevolezza dell'utente. La loro capacità di compromettere pressoché qualsiasi sistema operativo, sia iOS che Android, consente di accedere a informazioni altamente sensibili come messaggi, email, chiamate e persino comunicazioni cifrate. Tali caratteristiche pongono interrogativi sul pericolo che queste tecnologie vengano impiegate oltre i limiti stabiliti dal diritto, evolvendo da strumenti concepiti per la tutela della sicurezza nazionale

[1] NSO GROUP, in *https://www.nsogroup.com/about-us/*.

a veri e propri mezzi di sorveglianza di massa[2]. Come di recente sottolineato da un avvertimento ufficiale del Garante per protezione dei dati personali su Graphite, «le aziende che sviluppano tali sistemi sostengono di venderli solo a governi per scopi di sicurezza, ma numerosi casi hanno dimostrato come spesso finiscano nelle mani sbagliate, con conseguenze devastanti per le libertà individuali»[3].

Uno degli episodi più significativi legati all'impiego dello spyware Graphite, sviluppato dalla società israeliana Paragon Solutions, è rappresentato dallo scandalo internazionale emerso in seguito al suo utilizzo da parte di alcuni Stati per monitorare clandestinamente almeno novanta giornalisti e attivisti per i diritti umani in diversi Paesi[4]. L'episodio ha suscitato particolare allarme nella comunità internazionale, poiché ha messo in evidenza non solo la sofisticata capacità tecnica di tali strumenti di sorveglianza, ma anche le gravi implicazioni sul piano della libertà di stampa, della tutela della privacy e della protezione dei diritti fondamentali[5].

L'articolo si propone di analizzare l'impiego degli spyware mercenari (noti anche come spyware governativi o commerciali), mettendo in evidenza le loro caratteristiche tecniche e la capacità di trasformare dispositivi personali in strumenti di sorveglianza occulta. L'indagine si estende alla valutazione della legittimità del loro utilizzo nel quadro del diritto internazionale e delle convenzioni sui diritti umani, evidenziando i rischi di un impiego al di fuori dei confini legali, suscettibile di condurre a forme di sorveglianza illecita. In questo contesto, l'obiettivo

[2] Venice Commission, *Report on a Rule of Law and Human Rights Compliant Regulation of Spyware*, Consiglio d'Europa, 2024, (para.9); Amnesty International, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.

[3] Garante della protezione dei dati personali, *Paragon, Garante: "La sorveglianza è senza limiti: ecco il problema",* in AgendaDigitale, 2025.

[4] Amnesty International, *Caso Paragon: la Rete Diritti Umani Digitali chiede trasparenza, 2025, in https://www.amnesty.it/caso-paragon-la-rete-diritti-umani-digitali-chiede-trasparenza/.*

[5] Access Now, *Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan,* 2024, in *https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/#increased-use-of-spyware.*

è individuare soluzioni e misure di salvaguardia che consentano di bilanciare le esigenze di sicurezza con la tutela delle libertà fondamentali.

2. Lo spyware, secondo la definizione fornita dal Glossario del CSIRT Italia dell'Agenzia per la Cybersicurezza Nazionale è un «software malevolo in grado di "spiare" la vittima, in grado di raccogliere dati di varia natura (password, PIN, numero di carta di credito, dati di navigazione, ecc.) da computer e dispositivi e di trasmetterli successivamente a terze parti interessate al loro sfruttamento. La rilevazione degli spyware è spesso resa difficoltosa da tecniche di occultamento utilizzate dagli autori del software in fase di programmazione»[6]. La comprensione del funzionamento interno di uno spyware è essenziale per cogliere le ripercussioni che strumenti di sorveglianza, come Graphite e Pegasus, comportano in termini di sicurezza digitale e tutela della privacy. Tra le funzionalità più significative degli spyware si distinguono[7]:

- Controllo remoto: una volta installato, il software può essere gestito a distanza dall'attaccante, che ha la possibilità di impartire comandi e accedere ai dati presenti sul dispositivo.
- Zero-click exploits: questi spyware sfruttano vulnerabilità che non richiedono alcuna interazione da parte dell'utente per infettare il dispositivo, rendendo l'attacco estremamente difficile da rilevare e da prevenire.
- Operatività occulta: questi spyware sono concepiti per agire in modo invisibile, lasciando tracce minime. In alcuni casi possono anche autodistruggersi se rileva tentativi di analisi o rimozione.
- Estrazione dei dati: il malware è in grado di acquisire un'ampia gamma di informazioni, tra cui messaggi, email, contatti, registri delle chiamate e cronologia di navigazione. Può inoltre accedere ai contenuti di applicazioni di messaggistica cifrata come WhatsApp e Signal.

[6] Agenzia per la cybersicurezza nazionale, Glossario, in *https://www.acn.gov.it/portale/csirt-italia/glossario.*

[7] B. Marczak - J. Scott - Railton- B. Abdul Razzak - R. Deibert, *Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains, in (Citizen Lab Report n. 165),* University of Toronto, 2023.

- Sorveglianza audio e video: il software può attivare il microfono e fotocamera del dispositivo, consentendo la registrazione di audio e video senza che l'utente ne sia consapevole.
- Localizzazione in tempo reale: gli spyware sono capaci di tracciare la posizione geografica del dispositivo, permettendo di monitorare gli spostamenti esatti dell'utente bersaglio.
- Keylogging: il software può registrare i tasti digitati, rivelando così informazioni sensibili come password e credenziali di accesso.

Tra i principali vettori di attacco figurano certamente le tecniche di social engineering[8], come il phishing[9], e lo sfruttamento di vulnerabilità non note, i cosiddetti zero-day[10]. La crescente domanda di queste vulnerabilità alimenta un vero e proprio mercato globale degli exploit, nel quale broker specializzati acquistano e rivendono falle di sicurezza particolarmente apprezzate. Non sorprende, dunque, che le vulnerabilità più rare e potenti, come gli zero-click che consentono l'esecuzione di codice senza alcuna interazione dell'utente, raggiungano valori sempre più elevati anno dopo anno. Ad esempio, piattaforme come Zerodium arrivano a offrire ricompense nell'ordine di milioni di dollari per exploit zero-click in grado di compromettere dispositivi iOS o Android[11]. Tale dinamica contribuisce ad accrescere ulteriormente l'interesse della ricerca privata verso la scoperta di nuove vulnerabilità, che

[8] Agenzia per la cybersicurezza nazionale, Glossario: «Tecniche di manipolazione psicologica affinché l'utente compia determinate azioni o riveli informazioni sensibili come, ad esempio, credenziali di accesso a sistemi informatici».

[9] *Ibid*: «Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false email generiche a un gran numero di indirizzi. Le email sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Il phisher utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi».

[10] *Ibid*: «In gergo informatico, si intendono con zero-day (o 0-day) vulnerabilità riferite a sistemi, apparati e applicazioni non ancora note al produttore della tecnologia. La gravità degli zero-day è costituita dall'assenza di aggiornamenti software a fini di mitigazione (cd. patching). Proprio tali caratteristiche rendono gli zero-day oggetto di compravendite illecite da parte di soggetti intenzionati a sfruttarli per finalità intrusive».

[11] M. Dellago - A. C. Simpson - D. W. Woods, *Exploit Brokers and Offensive Cyber Operations, in The Cyber Defense Review,* vol. 7, no. 3, 2022, p. 36 ss.

alimenta un circolo vizioso che rafforza il mercato grigio delle vulnerabilità e, di conseguenza, aumenta i rischi complessivi per la sicurezza del cyberspazio e la tutela della privacy.

L'analisi degli episodi di utilizzo dello spyware Graphite, sviluppato dalla società israeliana Paragon Solutions, condotta dal Citizen Lab (laboratorio interdisciplinare con sede presso l'Università di Toronto, impegnato nella ricerca avanzata sull'impatto delle tecnologie sui diritti umani e sulla sicurezza globale)[12] ha fornito conferma forense che il malware sfruttava la vulnerabilità Apple CVE-2025-43200, una falla zero-day che consentiva l'esecuzione di un attacco zero-click tramite iMessage[13]. È significativo osservare che tale ricostruzione è stata possibile anche grazie alla collaborazione di Apple[14] e Meta che, attraverso i rispettivi team di sicurezza e di threat intelligence, hanno individuato attività anomale riconducibili alla catena d'infezione e hanno notificato agli utenti colpiti la compromissione dei loro dispositivi. In assenza di questo contributo coordinato, molte delle vittime non avrebbero avuto alcuna consapevolezza di essere state prese di mira da uno spyware mercenario.

In conclusione, spyware mercenari come Graphite e Pegasus rappresentano strumenti avanzati e altamente sofisticati, capaci di costituire una minaccia significativa per la tutela della sfera privata e delle libertà fondamentali. Le loro capacità estese, la natura furtiva e i molteplici vettori di infezione li rendono strumenti di sorveglianza formidabili, difficili da rilevare e contrastare. Sebbene siano disponibili diverse contromisure, la continua evoluzione del panorama delle minacce e le criticità strutturali del mercato delle vulnerabilità rendono evidente la necessità di un impegno coordinato tra governi, settore industriale e società civile per mitigare i rischi e garantire una tutela efficace della privacy e della sicurezza digitale dei cittadini.

[12] The Citizen Lab, *https://citizenlab.ca/about/.*

[13] B. Marczak - J. Scott-Railton *Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted, in Citizen Lab Report*, no. 186, 2025, University of Toronto.

[14] Apple, *Informazioni sulle notifiche di minaccia Apple e sulla protezione dallo spyware mercenario*, in *https://support.apple.com/it-it/102174.*

3. L'impiego di Graphite e di altri spyware mercenari solleva una molteplicità di questioni giuridiche che continuano a suscitare un intenso dibattito. Una delle preoccupazioni più rilevanti riguarda la tutela della privacy, tema che sarà approfondito nel paragrafo successivo. L'utilizzo di questi strumenti per attività di sorveglianza consente infatti di monitorare e raccogliere dati altamente sensibili senza che l'utente ne sia consapevole o abbia espresso il proprio consenso. Tale modalità operativa contrasta con numerose normative nazionali e internazionali, tra cui la Dichiarazione universale dei diritti umani, il Patto internazionale sui diritti civili e politici, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, la Convention 108+ e il Regolamento generale sulla protezione dei dati dell'Unione europea, che riconoscono la protezione della vita privata come un diritto fondamentale.

Accanto alle problematiche legate alla privacy, emergono casi documentati di sorveglianza illecita condotta attraverso spyware nei confronti di giornalisti, attivisti e oppositori politici. Questi episodi sollevano interrogativi particolarmente gravi, poiché possono violare norme che tutelano la libertà di espressione e di associazione, principi fondamentali degli ordinamenti democratici. Nell'era digitale, privacy e libertà di espressione risultano strettamente interconnesse, la protezione della sfera privata costituisce infatti una condizione imprescindibile per l'esercizio sicuro e libero della libertà di opinione e di espressione[15]. La natura pervasiva delle pratiche di sorveglianza può inoltre generare un effetto di autocensura, inducendo le persone a limitare le proprie comunicazioni o a evitare determinate attività per timore di essere monitorate[16]. Tale fenomeno rischia di incidere negativamente sul funzionamento delle società democratiche e sulla capacità delle persone di esercitare pienamente i propri diritti fondamentali.

[15] Nazioni Unite, Assemblea Generale, Consiglio dei diritti umani, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Un. Doc. A/HRC/41/35, 2019, p. 8.

[16] ARTICLE 19, *EU: Pegasus spyware Inquiry must hear the voices of human rights defend*ers, in *https://www.article19.org/resources/eu-pegasus-inquiry-must-hear-the-voices-of-human-rights-defenders/.*

Infine, anche il regime dei controlli sulle esportazioni contribuisce ad alimentare la discussione. Gli spyware sono classificati come tecnologie dual-use e sono pertanto soggetti al sistema di controllo previsto dal Wassenaar Arrangement[17], che disciplina l'esportazione e la diffusione di strumenti potenzialmente impiegabili sia in ambito civile sia per finalità militari[18]. Il Wassenaar Arrangement è un accordo multilaterale di controllo delle esportazioni tra Stati (attualmente 42 aderenti) volto a contribuire alla sicurezza e alla stabilità regionali e internazionali, promuovendo trasparenza e maggiore responsabilità nei trasferimenti di armi convenzionali e di beni e tecnologie dual-use. Sebbene la vendita e la distribuzione di prodotti come Graphite e Pegasus siano formalmente sottoposte a licenze di esportazione e regolamentazioni specifiche in diversi Paesi, resta controversa l'effettiva capacità di tali meccanismi di prevenire abusi e utilizzi impropri. La difficoltà nel tracciare la circolazione di queste tecnologie e nel garantire che vengano impiegate esclusivamente per scopi legittimi rappresenta una delle sfide più complesse nell'ambito della governance globale della sorveglianza digitale.

4. La definizione di garanzie contro le interferenze arbitrarie nella sfera privata si è affermata come un elemento essenziale del sistema internazionale di tutela dei diritti umani, divenuto ancor più centrale alla luce delle profonde trasformazioni che le tecnologie digitali stanno imponendo alle libertà individuali. I principali strumenti internazionali sanciscono il divieto di interferenze arbitrarie o illegittime nella vita privata dell'individuo. La Dichiarazione universale dei diritti umani del 1948 (d'ora in poi Dichiarazione), all'articolo 12, stabilisce che «Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella

[17] *Wassenaar Arrangements on Export Control for Conventional Arms and Dual-Use Goods and Technologies*, 1996, Participating States are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom and United States.

[18] L. Riecke, *Unmasking the Term 'Dual Use' in EU Spyware Export Control*, *in The European Journal of International Law*, vol. 34, no. 3, 2023, p. 704.

sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione»[19]. Analogo contenuto è previsto dall'articolo 17 del Patto internazionale sui diritti civili e politici del 1966 (d'ora in poi Patto), che vieta interferenze arbitrarie o illegittime nella vita privata e garantisce tutela giuridica contro tali attacchi[20]. Nel General Comment n. 16 relativo all'articolo 17 del Patto, il Comitato per i diritti umani ha precisato che la normativa interna deve definire in modo chiaro e puntuale le circostanze in cui sono consentite interferenze nella vita privata. Inoltre, ogni ingerenza deve essere autorizzata dall'autorità competente designata dalla legge e fondata su una valutazione individuale caso per caso[21].

Tra gli strumenti giuridici sviluppati nell'ambito del Consiglio d'Europa, un ruolo centrale è attribuito all'articolo 8 della Convenzione europea dei diritti dell'uomo del 1950 (d'ora in poi CEDU), che costituisce la disposizione di riferimento finalizzata a difendere l'individuo da ingerenze arbitrarie dei pubblici poteri e garantire il rispetto della vita privata e familiare e della propria corrispondenza[22]. Pur riconoscendo tali diritti, la disposizione ammette ingerenza da parte delle autorità pubbliche solo se «tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui»[23].

La protezione dei dati personali contenuti nei dispositivi elettronici assume oggi un ruolo particolarmente delicato nella salvaguardia della vita privata. Non vi è infatti dubbio che le informazioni archiviate in un dispositivo, incluse le comunicazioni telefoniche, rientrino pienamente

[19] Nazioni Unite, Risoluzione dell'Assemblea Generale, *Dichiarazione Universale dei Diritti Umani*, art. 12, 1948.

[20] Nazioni Unite, Risoluzione dell'Assemblea Generale, *Patto internazionale sui diritti civili e politici,* art. 17, 1966.

[21] Nazioni Unite, Comitato dei diritti umani, *General Comment No. 16: Article 17*, UN. Doc HRI/GEN/1/Rev.9 (Vol. I), 2008, p. 194, par. 8.

[22] Consiglio d'Europa, *Convenzione europea dei diritti dell'uomo*, Roma, art. 8, 1950.

[23] *Ibid.*, art. 8 comm. 2.

nelle nozioni di "vita privata" e di "corrispondenza"[24]. Proprio per questo, l'uso di spyware e strumenti di sorveglianza digitale costituisce dunque un'ingerenza diretta nel diritto alla privacy tutelato dall'articolo 8 CEDU, dall'articolo 17 del Patto e dall'articolo 12 della Dichiarazione. Tale ingerenza è ammissibile solo se soddisfa tre condizioni cumulative: a) deve essere chiaramente prevista dalla legge; b) deve perseguire uno degli scopi legittimi indicati dall'articolo 8 comma 2 della CEDU; c) risponde a un'esigenza sociale effettiva e risulta proporzionata allo scopo perseguito, così da potersi qualificare come necessaria in una società democratica[25]. Qualsiasi misura che non rispetti congiuntamente tali requisiti risulta incompatibile con la CEDU, anche quando sia diretta al perseguimento di obiettivi apparentemente legittimi.

In questa prospettiva, la Corte di Strasburgo, nella sentenza *Roman Zakharov v. Russia*[26], ha individuato una serie di garanzie minime che gli Stati devono prevedere per evitare abusi nell'adozione di misure di sorveglianza mirata: a) una chiara indicazione della natura dei reati che possono giustificare un ordine di intercettazione, b) la definizione delle categorie di persone che possono essere sottoposte a intercettazione, c) un limite alla durata dell'intercettazione, d) la procedura da seguire per l'esame, l'utilizzo e la conservazione dei dati ottenuti, e) le precauzioni da adottare nella comunicazione dei dati a terzi, f) le circostanze in cui le registrazioni possono o devono essere cancellate o distrutte. Inoltre, la Corte ha stabilito un obbligo di notifica al termine della misura di sorveglianza[27].

Considerato quanto precede, strumenti di sorveglianza come Pegasus e Graphite devono essere valutati alla luce dei principi ricavabili dagli articoli 12 della Dichiarazione, 17 del Patto e 8 della CEDU,

[24] CtEDU (Grande Camera), *Roman Zakharov c. Russia*, sentenza 4 dicembre 2015, ric. n. 47143/06, par. 173.

[25] Venice Commission, *Report on a Rule of Law and Human Rights Compliant Regulation of Spyware*, Consiglio d'Europa, 2024, para. 16.

[26] CtEDU (Grande Camera), *Roman Zakharov c. Russia*, sentenza 4 dicembre 2015, ric. n. 47143/06.

[27] Venice Commision, *Report on a Rule of Law and Human Rights Compliant Regulation of Spyware*, Consiglio d'Europa, 2024, para. 18.

i quali costituiscono oggi il parametro fondamentale per accertare la legittimità del loro impiego.

5. Questa ricerca ha analizzato gli spyware mercenari e le implicazioni legate alla legittimità del loro utilizzo nel quadro del diritto internazionale e delle convenzioni sui diritti umani. Sono state esaminate le capacità tecniche di strumenti avanzati come Graphite e Pegasus, il loro impiego da parte di diversi attori statali le controversie che ne sono derivate e le implicazioni legali che strumenti di sorveglianza così avanzati comportano per la privacy. La ricerca ha inoltre individuato soluzioni e misure di salvaguardia volte a bilanciare le esigenze di sicurezza con la tutela delle libertà fondamentali. L'esistenza e la proliferazione di spyware di nuova generazione hanno inoltre favorito l'espansione del mercato grigio degli exploit, incentivando la ricerca e la compravendita di vulnerabilità non conosciute.

Lo spyware rappresenta una tecnologia profondamente ambivalente. Se da un lato può rafforzare la sicurezza nazionale, dall'altro può essere facilmente impiegato per finalità arbitrarie, con effetti profondamente lesivi per la privacy. Osservando questa ambivalenza emerge con particolare evidenza il divario crescente tra l'evoluzione degli strumenti di indagine, sempre più potenti e capaci di penetrare ogni dimensione della vita digitale, e la stabilità del quadro internazionale di tutela dei diritti fondamentali. Le garanzie sancite dalle principali carte internazionali restano sostanzialmente immutate e continuano a offrire un riferimento solido, destinato ad applicarsi con efficacia anche alle tecnologie che ancora non conosciamo.

Tuttavia, a colpire maggiormente è la distanza tra l'esistenza di questo quadro di garanzie e la sua effettiva applicazione. Le norme ci sono, gli strumenti giuridici anche, eppure, la loro attuazione resta debole. La persistente reticenza dei governi nell'applicarle lascia il fianco a pratiche di sorveglianza invasive. Pretendere che la tecnologia non diventi un'arma contro la nostra libertà significa assumere, tutti, la responsabilità di vigilare affinché le garanzie esistenti diventino tutele reali.

ATTACKS ON CRITICAL INFRASTRUCTURES IN THE CONTEXT OF A CYBERWAR: ISSUES RELATING TO THE APPLICABILITY OF INTERNATIONAL LAW

Ilaria Infante

1. Nowadays, we are seeing more and more examples of hybrid warfare, which combines the traditional means of war with the cyber means provided by modern technology and usually directed against the critical infrastructures of a State.

Critical infrastructures can be defined as physical or virtual systems and assets that are so vital to a State that their malfunction or destruction would have a debilitating impact on national security, defence, economic stability and public health. Critical infrastructures are often managed by computer systems, including Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, also known as critical information infrastructures[1].

Attacks on critical infrastructures generally use the same technical means as other cybercrimes, with the difference that such attacks can have devastating effects on States, such as draining money from State treasuries or shutting down cities' water systems[2].

Therefore, depending on how they are carried out, attacks on critical IT infrastructure may be included among the various types of offences covered by the Budapest Convention[3], and the perpetrators of

[1] Council of Europe, Cybercrime Convention Committee (TC-Y), *TC-Y Guidance Note #6 : Critical Information Infrastructure Attacks*, TC-Y (2013)11E Rev, 5 June 2013, p. 3.

[2] *Ibid*.

[3] Council of Europe, *The Budapest Convention on Cybercrime*, European Treaty Series - No. 185, 23 November 2001.

such crimes may therefore be held criminally liable in accordance with the provisions of the relevant national legislation.

Nevertheless, given that, as mentioned above, the main goal of these attacks is to cause damage to a State, this may raise additional issues from the perspective of international law, since attacks on critical infrastructures could, in fact, be part of an ongoing cyberwar, that is a conflict between two or more States, or a State and a non-State entity, conducted primarily through cyber means and involving the use of computer systems, networks and the Internet for attack and defence.

Cyberwar should not be confused, however, with cyberwarfare, which is a broader term that refers to the use of digital means to achieve strategic objectives and may include cyberwar itself, as well as various other types of cyber operations, i.e. all the operations that can be carried out in cyberspace through the use of IT capabilities, such as, for example, espionage, sabotage, denial-of-service attacks, propaganda and information war[4]. Cyberwarfare, thus, typically refers to the techniques used during a cyberwar[5].

In light of the above, it emerges that a cyber attack to critical infrastructures could bring to the fore a series of rules and principles of international law[6].

The first issue to be resolved, however, concerns the applicability of international law to the context of cyberwar and cyber operations in general. In this regard, the so-called 'Tallinn Manual 2.0' (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations)[7] is particularly noteworthy, as it is a study drafted by 20 experts in international law at the invitation of the NATO Cooperative Cyber Defence

[4] New England Institute of Technology, *What Is a Cyber War - Explained*, 30 March 2023, available at *https://www.neit.edu/blog/what-is-a-cyber-war-explained.*

[5] Fortinet, *Cyber Warfare: The Expanding Battlefield of Nation-State Cyber Threats*, available at *https://www.fortinet.com/resources/cyberglossary/cyber-warfare.*

[6] For a more comprehensive analysis of the relationship between cyber operations in general and international law see for example: M. C. Vitucci, *Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo-ucraino*, in *La comunità internazionale*, vol. LXXVIII, 2023, pp.7-31.

[7] M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

Centre of Excellence, with the aim of analysing the application of international law to cyber operations. Even though the manual is not legally binding and is merely the result of the experts' opinion, it is recognised as a reference text on the subject, due to its ability to reinterpret international law and adapt it to the peculiarities of the cyberspace.

In the case of attacks on a State's critical infrastructures, the first rule of international law that comes to mind is undoubtedly the prohibition on the use of force, enshrined in Article 2, paragraph 4 of the United Nations (UN) Charter, and the related question of when a cyber operation could amount to an unlawful use of force under international law.

Furthermore, in a context characterised by anonymity such as the cyberspace, another fundamental issue is that of the attribution of a cyber operation, first to the single individual or group of individuals who carried it out and then, under international law, to a State who may have ordered it. In this regard, the Tallin Manual 2.0 also adopts the customary principles of international law relating to the responsibility of States for international wrongful acts and applies them to the case of cyber operations.

Therefore, this paper will focus on the analysis of the norms of international law that can apply to the case at hand, before concluding with a brief description of some practical examples of attacks against critical infrastructures, that could help to answer the questions of when a violation of the prohibition of the use of force occurs in the cyberspace, and if and when a hacker attack could be attributable to a State.

2. The main rule of international law that applies to the case of attacks on a State's critical infrastructure concerns the *jus ad bellum*, i.e. the rules governing the conditions under which a State may resort to armed force.

Under article 2, paragraph 4 of the UN Charter, in fact, «[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations»[8].

[8] UN Charter, art. 2, para. 4.

Based on this definition, Rule 68 of the Tallin Manual 2.0 establishes that «[a] cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful»[9]. Rule 69 of the Manual specifies, instead, that «[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force»[10].

Since, under international law, the term 'force' refers to armed force, this means that any cyber operation whose effects correspond to those produced by an armed attack will be considered prohibited. Therefore, cyber attacks on a State's critical infrastructure, that result in the injury or killing of people or in the physical damage or destruction of objects, constitute a use of force that is prohibited under international law.

The question of whether cyber operations can be equated with armed attacks is also relevant for the purposes of the applicability of the right to self-defence, since, as stated in Rule 71 of the Tallinn Manual 2.0, «[a] State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence»[11], and, therefore, respond in turn with the use of force, provided that this is necessary and proportionate. In addition, according to Rule 71, «[w]hether a cyber operation constitutes an armed attack depends on its scale and effects»[12].

The International Group of Experts that authored the Tallin Manual 2.0 unanimously concluded that certain cyber operations may be sufficiently serious to warrant classification as an 'armed attack' under the UN Charter[13]. This conclusion is consistent with the findings of the International Court of Justice (ICJ) in the *Nuclear Weapons Advisory Opinion*, according to which the UN Charter provisions relating to the

[9] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., Rule 68, p. 329.
[10] *Ibid.*, Rule 69, p. 330.
[11] *Ibid.*, Rule 71, p. 339.
[12] *Ibid.*
[13] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., p. 340.

use of force – and thus also article 51[14], which recognises the inherent right of self-defence against an armed attack – apply regardless of the means employed for the attack[15].

In any case, the ICJ had already emphasised, in the *Nicaragua v. United States* case, the need «to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms»[16], but it did so without providing further information on the matter. Therefore, the parameters relating to the criteria of scale and effects remain uncertain, beyond the indication that they must be grave[17].

Nevertheless, according to the International Group of Experts, it is clear that, for example, cases of «cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks»[18]. Conversely, they agreed that a cyber operation that seriously injures or kills a number of people or causes significant damage or destruction of property would satisfy the requirements of scale and effects[19].

According to other authors, however, even disruptive cyber operations could fall under the scope of Article 2, paragraph 4 of the UN Charter, if the disruption caused is significant enough to compromise

[14] UN Charter, art. 51: «Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security».

[15] ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226, para. 39.

[16] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986, p. 14, para. 191.

[17] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., p. 341.

[18] *Ibid.*

[19] *Ibid.*

the State security, or, more specifically, «"the safe and reliable functioning of 'critical infrastructure,' and the availability of 'key resources'"»[20].

In any case, as indicated in Rule 80 of the Tallin Manual 2.0, «[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict»[21], that is the so-called *jus in bello*, namely that particular branch of International Law, also known as International Humanitarian Law (IHL), which regulates wartime conduct and is primarily governed by the four Geneva Conventions[22] of 1949 and the two Additional Protocols[23] of 1977, in order to protect those who are not, or no longer, taking part in the hostilities.

For this reason, as recently highlighted by a Working Paper developed by various countries – including Brazil, Canada, Estonia, Germany, the Netherlands, Sweden and Switzerland – within the UN 'Open-ended Working Group on Security of and in the Use of Information and Communications Technologies', although there is no specific rule of IHL governing cyber operations, «[e]xisting IHL applies to and places important limits on cyber operations in the context of an armed conflict»[24], to the point that they must comply with the principles of military necessity, humanity, distinction and proportionality.

In particular, the principle of military necessity states that the only actions that can be taken are those that are actually necessary to achieve a legitimate military objective, which is solely to weaken the enemy's military forces[25]; the principle of humanity aims to limit and alleviate suffering and destruction during armed conflicts; the principle of

[20] M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2014, p. 55.

[21] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., Rule 80, p. 375.

[22] ICRC, *Geneva Conventions I, II, III and IV*, 12 August 1949.

[23] ICRC, *Additional Protocols I and II*, 8 June 1977.

[24] UN Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, *Working Paper on the Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflicts by Brazil, Canada, Chile, Colombia, the Czech Republic, Estonia, Germany, the Netherlands, Mexico, the Republic of Korea, Senegal, Sweden and Switzerland*, 9 July 2025, p. 2.

[25] *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight* (Saint Petersburg Declaration), 11 December 1868, preamble.

distinction provides the distinction between civilian population and combatants, as well as between civilian objects and military objects, according to which military operations may only be conducted against military targets[26]; and finally, the principle of proportionality prescribes that «an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated»[27] is strictly forbidden.

However, most of the rules derived from the principles of distinction and proportionality, which guarantee general protection for civilians and civilian objects, apply only to military operations that can be classified as 'attacks' according to IHL's definition, i.e. «acts of violence against the adversary, whether in offence or in defence»[28].

When it comes to cyberspace, according to Rule 92 of the Tallin Manual 2.0 «[a] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects»[29]. It is widely recognised, in fact, that cyber operations that could cause death, injury or physical damage constitute attacks under IHL. According to the International Committee of the Red Cross, this includes damage due to the foreseeable direct and indirect effects of an attack, such as the death of patients in intensive care caused by a cyber operation on an electricity network that results in the power supply to a hospital being cut off[30].

Even according to the experts that participated in the 'Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector' – as IHL requires that medical units, transport and medical personnel be respected and protected at all time – parties involved in armed conflicts: «must not disrupt the functioning of health-care facilities through cyber operations; must take all feasible

[26] *Additional Protocol I*, art. 48.

[27] *Additional Protocol I*, art. 51, para. 5, let. b.

[28] *Additional Protocol I*, art. 49, para. 1.

[29] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., Rule 92, p. 415.

[30] ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, ICRC position paper, November 2019, p. 7.

precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations»[31].

However, there are differing views on whether a cyber operation that results in a loss of functionality without causing physical damage can be classified as an attack under IHL.

For example, although some of the experts involved in the Tallinn Manual 2.0 expressed a negative opinion, the majority of them were of the view that interference with functionality qualifies as damage only if restoring functionality requires the replacement of physical components[32]. Other experts, instead, have argued that interference with functionality also extends to situations where the operating system or the specific damaged data needs to be reinstalled, emphasising that if, following a cyber operation that deletes or alters data, the infrastructure cannot perform its originally intended function, the operation in question constitutes an attack[33].

3. Another issue of fundamental importance from the point of view of international law is that of responsibility. Since cyber attacks always originate from individuals, such as hackers, in fact, this raises the question of attributing their actions to a State for the purposes of international responsibility.

In this regard, following the principles enshrined in Articles 4 and 5 of the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA)[34], the Tallinn Manual 2.0 states, in Rule 15, that «[c]ber operations conducted by organs of a State, or by persons

[31] *Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector*, para. 5, available at *https://www.ejiltalk.org/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/*.

[32] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., p. 417.

[33] *Ibid.*, pp. 417-418.

[34] ILC, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, UN Doc. A/56/10, 2001, arts. 4,5.

or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State»[35].

The issue becomes more complex when the cyber operations are carried out by private entities that are not organs of a State. In this case, in line with Articles 8 and 11 of the ARSIWA[36], Rule 17 of the Tallinn Manual 2.0 maintains that «[c]yber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own»[37].

The Tallinn Manual uses the term 'non-State actors' to refer to both individuals and groups, including, for example: individual hackers; informal groups such as Anonymous; criminal organisations involved in cybercrime; legal entities such as IT, software and hardware companies; and cyberterrorists[38].

What matters, for the purposes of international law, is that such entities act on the instructions of the State or under its control, which, as recognised by the ICJ on several occasions[39], must be an effective control.

A State has 'effective control' of a particular cyber operation by a non-State actor whenever the State determines the execution and course of the specific operation and the cyber activity carried out by the non-State actor is an integral part of that operation[40].

Therefore, as exemplified by the Tallinn Manual 2.0, if a State instructs a private company, which provides support to its armed forces, to undertake a cyber operation that violates the State's international obligations towards another State, then that cyber operation is attributable to the State in question. For example, if the State orders the company to conduct operations against the SCADA system of another

[35] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., Rule 15, p. 87.

[36] *Articles on Responsibility of States for Internationally Wrongful Acts*, arts. 8,11.

[37] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., Rule 17, p. 94.

[38] *Ibid*., p. 95.

[39] See for example ICJ: *Nicaragua v. United States*, para. 115; and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, p. 43, para. 401.

[40] M. N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., p. 96.

State, in order to destroy its assets and property, and the company introduces a destructive logic bomb (a type of malware) into the system in question, causing serious damage to critical infrastructures in that particular State, then the conduct is attributable to the State that ordered it[41].

When it comes to hacker groups, however, given the typical two-tier structure that characterises the majority of them, the State will probably have to establish close ties with the upper tier of this structure or directly join it with its own agents. Only then could the State issue specific directions about the conducts – like providing target lists or indicating particular objectives – which, through the filter of the group's upper level, would reach all the members[42].

In practice, though, attributing the cyber conduct of non-State actors to the State can prove to be particularly difficult, especially for technical reasons. The opacity of the web and the volatility of digital evidence can hinder the ability to prove the connection with the State or even to determine the origin of the attack itself. In fact, since any instructions, directives or control from the State are likely to be mostly in digital format, they could be easily and quickly deleted or altered. Technical traceability issues, potentially exacerbated by the transnational nature of the attack, which may originate in different jurisdictions, and the use of obfuscation methods, may also combine with issues of inter-State cooperation as, when assessing the origin of the attack, the attacked State may need assistance from the countries where the attack originated, or where the physical devices were located[43].

All of this makes it even more difficult to attribute the cyber attack to a State for the purposes of international responsibility, since identifying who is behind a cyber operation presents considerable technical issues, due to the prevalent anonymity of cyberspace. However, some instruments like traditional intelligence gathering and cyber exploita-

[41] *Ibid.*, pp. 97-98.

[42] N. Bussolati, *The Rise of Non-State Actors in Cyberwarfare*, in *Cyber War: Law and Ethics for Virtual Conflicts*, J. D. Ohlin - K. Govern - C. Finkelstein (eds.), Oxford University Press, 2015, pp. 120-121.

[43] *Ibid.*, p. 121.

tion, as well as traceback technical tools, could help to eventually identify the author of a cyber operation[44].

Once the authors are identified, attribution under the law of State responsibility becomes «the key to understanding the motive of an attack and consequently being able to differentiate between a criminal act and warfare in cyberspace»[45].

4. Concrete examples of cyber attacks against critical infrastructure include the Stuxnet case and the various attacks carried out in the context of the hybrid war between Russia and Ukraine.

In particular, the Stuxnet case, which became known in 2010, concerned a cyber campaign, called 'Operation Olympic Games', which the United States, with the support of Israel, had launched against Iran to disrupt its nuclear programme, by targeting the gas centrifuges at the Natanz uranium enrichment plant.

Unlike other malware, the worm did not just replicate itself, but also contained a 'weaponised' payload designed to give instructions to other programmes. It is, in fact, the first known use of malicious software designed to cause physical damage by attacking the SCADA system of a critical national infrastructure[46]. A payload is a routine present in a computer virus that extends its functions beyond infecting the system. In short, these are the actions that the virus performs after infecting the system. Payload therefore refers to any time-limited, random or trigger-activated operation that a virus or worm executes. This may involve partial or total destruction of information.

In this specific case, the worm destroyed almost a fifth of Iran's nuclear centrifuges, infected over 200,000 computers and caused physical damage to 1,000 machines. In particular, Stuxnet searched every infected computer for traces of the Siemens Step7 Factory System (SCADA) software, used by industrial computers that act as Programmable Logic Controllers (PLCs) to automate and monitor electromagnetic

[44] M. Roscini, *Cyber Operations and the Use of Force*, cit., p. 33.

[45] E. Keymer, *The cyber-war*, in *Jane's Defence Weekly*, n. 47/39, 29 September 2010, p. 22.

[46] M. Roscini, *Cyber Operations and the Use of Force*, cit., p. 6.

equipment. Once it found this software, Stuxnet began updating its code to send destructive instructions to the electromagnetic equipment controlled by the computers[47].

Circumstantial evidence about the involvement of the United States included the fact that the worm had mainly affected Iran and specifically targeted the Natanz nuclear facility, as the worm only activated when it found the Siemens software used in that facility, and the fact that the high sophistication of the attack, the use of several zero-day hacks and the in-depth knowledge of the targeted system required resources not normally available to individual hackers[48].

As for the war in Ukraine, it has been described as «the first major conflict to feature large-scale cyber operations»[49], with «Russia's use of hybrid warfare techniques […] – particularly cyber operations – [being] unprecedented in scope and scale»[50].

Since 2014, in fact, Russian hackers have launched a series of attacks against Ukraine's critical infrastructures, such as the repeated attacks on Ukrainian electricity grids in 2015-2016, as well as more recent attacks during the escalation of the war in 2022[51]. These attacks involve the use of various wipers and malware to destroy critical data, disrupt communication systems, such as satellites, and prevent access to the Internet for thousands of civilians, damaging – sometimes beyond repair – Ukraine's critical infrastructures[52].

Other examples of cyber operations where the Russian Federation was considered responsible were the distributed denial-of-service

[47] Kaspersky, *Stuxnet explained: What it is, who created it and how it works*, available at *https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet*.

[48] M. Roscini, *Cyber Operations and the Use of Force*, cit., p. 217.

[49] J. A. Lewis, *Cyber War and Ukraine*, Center for Strategic & International Studies, 16 June 2022, available at *https://www.csis.org/analysis/cyber-war-and-ukraine*.

[50] FP Analytics, *The Evolution of Cyber Operations in Armed Conflict*, available at *https://digitalfrontlines.io/2023/05/25/the-evolution-of-cyber-operations-in-armed-conflict/*.

[51] K. Chan Yoon Onn, *The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine): Some Preliminary Reflections*, EJIL:Talk!, 15 September 2023, available at *https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-the-international-criminal-court-and-its-implications-for-ukraine-some-preliminary-reflections/*.

[52] *Ibid.*

(DDoS) attacks against Estonia in 2007 and the cyber attacks against Georgia in 2008.

In particular, in the case of Estonia, even if the cyber operations did not breach the prohibition of the use of force, since the targeted critical infrastructures, like banks and communications, were not physically destroyed nor seriously disrupted, the DDoS attacks had been conclusively attributed to Russia[53]. This was due to the fact that the hackers claimed to be Russian, that the tools used to hack and deface websites were found on Russian websites and chat rooms, and that the attacks were launched on 9 May – which is the day on which Russia celebrates Victory Day in Europe in the Second World War – against the backdrop of the removal of a Russian war memorial from the centre of Tallinn. Moreover, although the botnets included computers located in several countries, it appears that at least some attacks originated from Russian IP addresses, including those belonging to State institutions, and that, in any case, they required resources not available to ordinary people[54]. On the other hand, the cyber attacks against Georgia began immediately before and continued throughout the August 2008 Russo-Georgian conflict, which led to the *de facto* separations of Abkhazia and South Ossetia from Georgia. As in the case of Estonia, it has been reported that «the Russian hacker community was involved in the cyber attacks and that coordination took place in the Russian language and in Russian or Russian-related fora»[55]. Likewise, it was argued that the level of coordination and preparation suggested the support of the government, and, finally, it was found that IP addresses belonging to Russian State-run companies were used to launch the attacks[56].

In conclusion, the brief analysis of these few practical cases of cyber attacks against critical infrastructures helped us to better understand what has been explained in the precedent paragraphs. Indeed, it has become evident that when a cyber attack results in the physical damage of the target hit then we can consider it as an attack in the meaning

[53] M. Roscini, *Cyber Operations and the Use of Force*, cit., p. 63.
[54] M. Roscini, *Cyber Operations and the Use of Force*, cit., p. 216.
[55] *Ibid.*
[56] *Ibid.*

of international law, such as in the case of Stuxnet where the machines operating in the Iranian nuclear facility were physically destroyed by the virus. Moreover, as the examples described demonstrated, in order to answer the difficult question of if and when a cyber attack could be attributable to a State, elements like the high sophistication of the attacks, the use of resources not available to ordinary hackers and the traceback of the IP from which the attacks originated to State institutions, are useful instruments in proving that there had been a State involvement in the cyber operation to the point that the action could be attributable to it under international law.

LA DIMENSIONE CIBERNETICA DEI REATI CONTRO IL PATRIMONIO: ALCUNE RIFLESSIONI IN TEMA DI CHEATING INFORMATICO

Federica De Simone

1. Nell'ecosistema digitale attuale i confini delle minacce cibernetiche si stanno ampliando sempre più, sino ad occupare spazi un tempo impensabili, ma da ritenersi già superati non appena immaginati.

La sofisticazione *in crescendo* delle nuove tecnologie dà luogo a una casistica in continua evoluzione, i cui disparati profili di offensività costringono il penalista a un'interpretazione ermeneutica frammentaria nell'attesa che le categorie dogmatiche tradizionali siano ripensate in chiave funzionale. Tali fenomeni, infatti, destano un significativo allarme sociale, non solo per i rischi di lesione dei diritti fondamentali del singolo, ma anche per la dimensione sistemica che tali minacce possono assumere e che ben possono incidere sulla tenuta dell'apparato ordinamentale. La criticità emerge in maniera ancora più evidente ove si consideri la sproporzione tra le azioni dei cyber criminali e coloro che sono chiamati a difendersi, siano essi attori statali o attori privati. Mentre i primi, infatti, si limitano a individuare e sfruttare le vulnerabilità dei sistemi informatici altrui colpendo i punti di accesso esposti, le vittime sono chiamate a porre in campo una risposta ben più ampia che contempli strategie difensive molteplici atte a coprire un vasto perimetro[1].

[1] Sul punto la bibliografia è vasta, per tutti si veda W. Ibrar (et al.), *Generative AI: a double-edged sword in the cyber threat landscape*, in *Artificial Intelligence Review*, 2025, 58, p. 285 ss.; R. Anderson, *Security Engineering. A Guide to Building Dependable Distribuited Systems*, ed. Wiley, John Wiley & Sons Inc, 2021.

Nel panorama delle frodi in senso ampio, l'eterogeneità delle forme di aggressione è tale da includere sia ipotesi di vera e propria manipolazione delle vittime e/o degli strumenti informatici, sia forme di intrusione che si traducono in vulnerabilità e finanche compromissione degli apparati tecnologici. In particolare, basti pensare ai casi comunemente definiti di *social engineering* in cui l'inganno è di natura psicologica e realizza – sotto il profilo teorico – un imbroglio che in gergo si definisce *cheating*.

Come si approfondirà nel prosieguo, si tratta di fattispecie caratterizzate da una diversità composita sotto il profilo strutturale, da riferirsi sia alle differenti modalità di condotta sia agli effetti prodotti in termini di evento finale, ma che – al contempo – hanno in comune l'oggetto della tutela. La collocazione sistematica all'interno del codice penale, infatti, indirizza l'interprete verso i reati contro il patrimonio in cui emerge la natura predatoria delle condotte, finalizzate al conseguimento di un ingiusto profitto con altrui danno[2]. Cionondimeno, l'operazione di sussunzione delle nuove ipotesi a fattispecie astratte classiche e la conseguente ricostruzione esegetica del bene giuridico in termini dommatici, non mette al riparo da evidenti aporie di sistema. Invero, i reati contro il patrimonio fanno leva sul paradigma ontologico della materialità, tanto quanto la maggior parte dei *cybercrime* restituisce una dimensione di immaterialità, derivando da questa relazione inversamente proporzionale un primo punto evidente di frizione nel rischio di un'indebita dilatazione dei requisiti di tipicità[3].

Il presente contributo si propone, dunque, di analizzare i tratti essenziali della fattispecie di frode informatica, anche indagando l'opportunità di equiparare espressamente il patrimonio informatico (in qualità di bene giuridico di nuova emersione) al patrimonio inteso in senso stretto.

[2] S. Moccia, *Tutela penale del patrimonio e principi costituzionali*, Cedam, 1988, pp. 30 ss., secondo cui l'attuale tutela penale del patrimonio, accogliendo ancora una concezione tardo ottocentesca incentrata sulla proprietà della 'cosa', è da considerarsi anacronistica.

[3] Si veda E. Mazzantini, *La tutela del patrimonio alla prova della smaterializzazione dei rapporti socio-economici. La centralità dei delitti di frode nel sistema penale "vivente"*, in *Riv. it. dir. proc. pen*., 2020, 1, pp. 75 ss. La criticità era già stata sollevata da V. Militello, *Patrimonio (delitti contro il)*, in *Digesto pen.*, 1995, IX, p. 278 ss.

2. Tradizionalmente, l'oggetto materiale dei reati contro il patrimonio è la cosa mobile[4], in merito alla quale un primo spunto di riflessione è offerto dalla tradizione romanistica, che distingue i cosiddetti *nomina appellativa* in *res corporalis* e *res incorporalis*, a seconda che *videri tangique possunt*, ovvero *tangi non possunt*[5].

Ai fini del discorso, la risalente distinzione sembra assumere centrale rilevanza in relazione soprattutto a un recente arresto giurisprudenziale che sul punto pone alcuni profili di criticità, lasciando irrisolta la questione in merito alla tutela di beni immateriali come quelli digitali. Nel caso Carluccini[6], infatti, la Suprema Corte ha ritenuto suscettibile di appropriazione indebita il file informatico, ribaltando il consolidato orientamento[7] secondo cui un bene immateriale non può essere oggetto di sottrazione. La giurisprudenza di legittimità, compiendo un salto logico, ha operato un'interpretazione estensiva del concetto di cosa mobile alla nozione di dato informatico. Il ragionamento prende le mosse dalla considerazione che il file, ancorché non percepibile dai sensi, è pur sempre dotato di una dimensione fisica rilevabile tramite la misurazione dello spazio che occupa all'interno del supporto informatico, tanto più che può essere oggetto di trasferimento[8].

[4] *Ex multis*, G. Petragnani Gelosi, *I delitti di furto*, in A. Cadoppi - S. Canestrari, A. Manna - M. Papa (diretto da), *Diritto Penale*, Utet, 2022, III, p. 6851 ss. Sul concetto di 'cosa' si veda A. Pagliaro, *Appropriazione indebita*, in *Digesto pen*., 1987, p. 225 ss; S. Pugliatti, voce *Cosa in senso giuridico (teoria generale)*, in *Enc. dir*., 1959, XII, p. 19 e ss.

[5] Ampiamente G. Nicosia, *Possessio e res incorporales*, in A.a.V.v., *Annali del Seminario Giuridico dell'Università degli Studi di Palermo* (AUPA), Giappichelli, 2013, LVI, p. 275 ss.; G. Turelli, *'Res incorporales' e 'beni immateriali': categorie affini, ma non congruenti*, in *Teoria e Storia del diritto privato*, 2012, 5, p. 7 ss.

[6] Corte Cass. Sez. II, sentenza 7 novembre 2019 n. 11959, con nota di L. Barile, *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia il diritto penale è 'cosa mobile*, in *Sist. Pen*., 2021, 3, p. 139 ss.

[7] Cass. pen. Sez. IV, sentenza 21 dicembre 2010 n. 44840 a conferma di Cass. pen. Sez. IV, sentenza13 novembre 2003 n. 3449.

[8] La ricostruzione operata nella sentenza prende in considerazione la nozione tecnico-scientifico di file, anziché ricorrere al significato letterale proprio del sistema giuridico. Non è questa la sede per approfondire i tratti salienti della sentenza citata, si rinvia a C. Deflorio, *La qualificazione del file come "cosa mobile" suscettibile di essere oggetto di furto*, in *Crit. Dir*., 1 giugno 2021, in *https://rivistacriticadeldiritto.it/?p=1716#_ftnref11*; N. Pisani, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, in *Dir. pen. proc*., 2020, 5,p. 651 ss.

Benché di primo acchito la soluzione offerta dal formante giurisprudenziale possa sembrare dirimente, essa non trova una corrispondenza nel formante legislativo, per il quale – invece – i beni immateriali ancora oggi non rientrano nella nozione di cose mobili[9]. Tant'è vero ciò che le ipotesi in cui si osserva una smaterializzazione sono frutto di una circoscritta scelta di politica criminale e sono avvertite come eccezioni che confermano la regola. Basti pensare al dettato dell'art. 624 co. 2 c.p., che equipara l'energia elettrica alla cosa mobile solo in quanto dotata di valore economico e potenzialmente oggetto di sottrazione con conseguente *profitto proprio e danno altrui*[10]. Pur esulando dai reati contro il patrimonio, un discorso simile ha trovato applicazione per il concetto di domicilio informatico, la cui tutela è pacificamente affidata all'art. 615 *ter* c.p., quant'anche la norma non contenga un espresso riferimento in tal senso se non in virtù della collocazione sistematica[11]. Dunque, vale sempre la considerazione che se il legislatore avesse voluto regolare in tal senso la materia, ben avrebbe potuto esplicitare la scelta nei numerosi interventi che dal 1993 si sono susseguiti in tema di reati informatici.

Non solo il dato normativo non offre un valido addentellato alla posizione della Corte, ma anche la dottrina non sembra avallare la con-

[9] La *ratio legis* sottesa al dato normativo trova un autorevole dentellato dottrinario in M. Romano, *I delitti contro la Pubblica Amministrazione. I delitti dei pubblici ufficiali*, in *Comm. Sist.*, 2019, p. 24 ss., secondo cui è 'cosa mobile' qualsiasi «*cosa corporale, fungibile o infungibile, idonea a essere trasportata come tale, ovvero secondo la sua ordinaria funzione*». In tal senso anche F. Antolisei, *Manuale di diritto penale. Parte speciale*, vol. I, Milano, 2016, 382; G. Fiandaca - E. Musco, *Diritto Penale. Parte speciale. I delitti contro il patrimonio*, Zanichelli, 2015, p. 29 ss.

[10] Si vedano i *Lavori preparatori del codice penale e del codice di procedura penale. Progetto definitivo di un nuovo codice penale con la relazione del guardasigilli On. Alfredo Rocco*, Roma 1929, V, II, pp. 439 ss. in *https://www.giustizia.it/cmsresources/cms/documents/cp_49_5_2_prog_defin_relaz_libri_23_1929.pdf.*

[11] L'art. 615 *ter* c.p., introdotto dall'art. 4 della l. 23 dicembre 1993 n. 547 nell'ambito dei delitti contro la libertà individuale, punisce l'accesso abusivo a un sistema informatico o telematico, articolandolo proprio sulla falsariga dell'art. 614 c.p. Tuttavia, anche in questa ipotesi è la giurisprudenza che espressamente ha fatto riferimento al concetto di domicilio informatico, non essendoci alcun esplicito riferimento in tal senso nella rubrica della citata norma ed essendo la riservatezza informatica il bene giuridico tutelato. Si veda I. Salvadori, *I reati contro la riservatezza informatica*, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (diretto da), *Cybercrime*, Wolters Kluwer Italia, 2022, p. 656 ss.

clusione. Si obietta, *in primis*, che una simile ricostruzione non tiene in debito conto la distinzione tra file e dato, potendosi riferire la materialità solo al primo. Questo, infatti, assume le vesti di un vero e proprio contenitore, la cui fisicità è espressa dal supporto elettromagnetico e che può essere misurato, spostato, copiato e cancellato. Il dato, invece, coincide con l'informazione contenuta nel file ed è totalmente privo di un sostrato di tangibilità materiale. La distinzione non è meramente formale, ma involge la possibilità stessa di ascrivere una seppure minima forma di fisicità alla *res digitalis*, mettendo in crisi anche i tradizionali requisiti di spossessamento e sottrazione richiesti, ad esempio, per le ipotesi di furto o appropriazione indebita, a prescindere dalla circostanza che il titolare ne mantenga la disponibilità[12].

Stando così le cose, la soluzione giurisprudenziale non darebbe luogo a una forma di interpretazione estensiva, bensì costituirebbe una vera e propria ipotesi di analogia *in malam partem*, in cui l'applicazione della disciplina dettata per la *res corporalis* alla categoria della *res digitalis* non inclusa nella previsione normativa, superando il perimetro della fattispecie tipica, si traduce in una violazione del principio di legalità[13].

Prova ne sia il successivo *revirement* della stessa Corte[14], che nel 2022 ha ritenuto non integrato il reato di appropriazione indebita in un caso di copiatura di file informatico. Sebbene nel caso di specie si osservi che la mancanza del requisito dello spossessamento sia dovuto al fatto che si tratti di una ipotesi di copiatura e non di cancellazione, l'elemento materiale difetterebbe comunque. La Corte chiarisce, infatti, che la dimensione spaziale del *file* espressa in *byte* costituisce solo una forma di manifestazione dell'informazione, rimanendo quest'ultima un bene immateriale distinto, come tale non assimilabile alla cosa mobile.

Decaduta la possibilità di rinvenire un *minimum* di fisicità e non potendosi, altresì, ritenere integrati i requisiti della definibilità di uno

[12] Nel caso *Carluccini*, invero, i giudici hanno ritenuto configurata l'ipotesi dell' appropriazione indebita proprio in considerazione del fatto che il file era stato oggetto di cancellazione e, dunque, non era più nella disponibilità del proprietario. *Contra* F. Mantovani, *Diritto penale. Delitti contro il patrimonio*, Cedam, 2021, p. 24.

[13] Sul divieto di analogia G. Marinucci, *L'analogia e la punibilità svincolata dalla conformità alla fattispecie penale*, in *Riv. it. dir. proc. pen.*, 2007, 4, p. 1254 ss.

[14] Cass. pen. Sez. II, sentenza 12 luglio 2022 n. 26899.

spazio e della suscettibilità di uno spostamento materiale, oltre che della possibilità di realizzare uno spossessamento in senso stretto, l'esigenza di individuare una soluzione impone di esplorare altre strade. Ciò è reso indefettibile dalla presa di coscienza del mutato contesto di riferimento, in cui lo sviluppo tecnologico rende sempre più evidente il processo di smaterializzazione della ricchezza e, al contempo, l'aumento del valore patrimoniale della *res digitalis*.

A tal punto, sembrano delinearsi due alternative. La prima, prendendo le mosse dal superamento della radicata equivalenza cosa mobile/*res corporalis*, dovrebbe portare a un ripensamento *in toto* della dimensione di stretta materialità che caratterizza i reati contro il patrimonio, prediligendo un criterio connesso al valore astratto del bene. Si colmerebbero, così, le lacune normative, tra cui quella che impedisce di tutelare il file informatico nei casi di furto, garantendo al tempo stesso il rispetto del principio di tassatività e determinatezza.

La seconda opzione, lasciando intatti i paradigmi tradizionali previsti per le ipotesi classiche, porterebbe all'introduzione di una disciplina specifica per il mondo digitale che, anche per il tramite dell'adozione di un Testo Unico, possa garantire una tutela *ad hoc*, proprio riconoscendo concetti come quello del patrimonio informatico e della *res digitalis*.

La prima soluzione, pur implicando un intervento di natura radicale, lascia in parte impregiudicate le criticità osservate. L'espansione interpretativa della materialità, infatti, pur abbandonando la dimensione della fisicità a favore del diverso e più fluido concetto di 'valore', impone una delimitazione puntuale sotto il profilo normativo, affinché sia possibile circoscrivere la sfera applicativa. Diversamente, si correrebbe il rischio di una riforma che potrebbe addirittura amplificare il problema dell'indeterminatezza, come a dire … il rimedio è peggio del male.

Sul piano del rispetto dei principi fondamentali e di una coerenza di sistema in generale, sembra preferibile la seconda opzione. Un intervento normativo specifico garantirebbe, infatti, il rispetto del principio di legalità in tutte le sue accezioni, con particolare riguardo – appunto – al principio di tassatività e determinatezza e al divieto di analogia, garantendo la certezza del diritto. L'introduzione di fattispecie connotate da un alto tasso di specificità tecnica, permetterebbe al tempo stesso

di colmare quelle lacune che gli interventi normativi susseguitisi nel tempo non sono riusciti a risolvere, evitando – così – pericolosi vuoti di tutela.

3. Di fronte al dilagare dei casi di *cybercrime* e nel tentativo di apprestare una qualche forma di tutela al patrimonio informatico[15], il legislatore ha, dapprima, introdotto il delitto di frode informatica e, solo recentemente, quello di estorsione informatica. Certo l'ampia distanza temporale tra i due interventi normativi testimonia sia la necessità di stare al passo con una tecnologia in continua evoluzione, sia la difficoltà di estendere le fattispecie classiche alle nuove ipotesi, avvalorando la tesi per cui sarebbe opportuno adottare una normativa di settore.

La mancanza di una disciplina organica in materia e la crisi del paradigma materialistico concorrono a indebolire fortemente tale tutela, soprattutto ove si consideri l'assenza di una disciplina atta a sanzionare le ipotesi di sottrazione della *res digitalis*. L'impossibilità di contestare gli elementi tipici della sottrazione e dell'appropriazione nel caso del file costituisce un rilevante *vulnus*. Tali condotte, infatti, sono prodromiche e maggiormente ricorrenti proprio nei casi di frode ed estorsione informatica, soprattutto quando queste assumono le forme del *cheating* e del *ransomware*. Basti pensare alla frequenza con cui queste ipotesi sono precedute dalla sottrazione di credenziali o dati personali, che oggi può essere contestata solo ove integri gli elementi tipici dell'accesso abusivo (art. 615 *ter* c.p.) o del danneggiamento informatico (art. 635 *bis* c.p.).

[15] Invero, il riconoscimento del patrimonio informatico *ex se* va inteso in maniera atecnica, mancando un espressa previsione normativa in tal senso. Tuttavia, sul punto il dibattito in dottrina è acceso. Da un lato, i sostenitori del patrimonio in senso funzionalistico, che sostengono la concezione classica del patrimonio, anche in virtù della collocazione codicistica. Dall'altro, coloro che accolgono un orientamento più moderno, elevando a bene giuridico l'integrità dei dati, programmi e sistemi informatici. Per i primi si veda G. Pica, *Diritto penale delle tecnologie informatiche*, Utet, 1999, p. 86 ss.; L. Scopinaro, *Internet e reati contro il patrimonio*, Giappichelli, 2007, p. 206; G. Fiandaca, E. Musco, *Diritto penale. Parte speciale*, cit., p. 145; F. Antolisei, *Diritto penale. Parte speciale*, Giuffrè, 2022, I, p. 604 ss. Nel solco del secondo orientamento, I. Salvadori, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. proc. pen.*, 2012, 1, p. 204 ss.

La sanzione del solo segmento finale di tutto l'*iter criminis*, corrispondente alla realizzazione della frode o dell'estorsione, sembra deporre per una tutela differenziata del patrimonio informatico rispetto a quello inteso in senso tradizionale, in cui non tutte le offese sono oggetto di una risposta ordinamentale. La scelta operata dal legislatore di una tutela frammentaria appare distonica non solo rispetto alla portata fenomenologica, ma anche in riferimento all'evento di danno caratterizzante queste fattispecie e che appare anch'esso oggetto di una sorta di dematerializzazione. Il danno patrimoniale, infatti, non si esaurisce nella sola perdita diretta di denaro, ma comprende altresì la compromissione dei sistemi informatici oggetto dell'attacco e la perdita della titolarità o dell'esclusività dei dati. Ne consegue che anche il profitto assume una veste diversa, non esaurendosi nel conseguimento di una somma di denaro, ma ben potendo comprendere beni di natura diversa, quali la reputazione, la possibilità di gestire un flusso informativo e finanche lo stesso vantaggio tecnologico. Sembra, allora, riduttiva una lettura del danno alla luce del solo parametro patrimoniale di natura economica, vantando il patrimonio informatico una dimensione ben più ampia che travalica – appunto – la sfera economica del soggetto. La sottrazione di dati informatici, ad esempio, potrebbe non avere una ricaduta in tal senso sulla vittima, soprattutto nel caso in cui non ci sia la cancellazione, ma solo la copiatura; lo stesso potrebbe verificarsi per alcuni casi di danneggiamento (artt. 635 *bis* e ss. c.p.), per i quali l'eventuale perdita di operatività potrebbe essere difficile da quantificare in termini economici[16].

4. Il riconoscimento, seppure non espresso, dell'esigenza di tutela del patrimonio informatico emerge in maniera evidente dall'introdu-

[16] Parte della dottrina riconosce il carattere della plurioffensività in capo ad alcuni reati informatici. Nella frode informatica, ad esempio, la tutela si estenderebbe anche al corretto funzionamento dei sistemi informatici e della riservatezza che deve caratterizzare l'utilizzazione di tali sistemi. Cfr. G. Fiandaca - F. Musco, *Diritto penale. Parte speciale II. I delitti contro il patrimonio*, Zanichelli, 2012, p. 198. Più recentemente, M. Santise - F. Zunica, *Il diritto penale del web*, in *Coordinate ermeneutiche di diritto penale*, Giappichelli, 2021, p. 888; G. Minicucci, *Le frodi informatiche*, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (diretto da), *Cybercrime*, cit., p. 827 ss.

zione dell'art. 640 *ter* c.p. nel lontano 1993, anno in cui – a seguito di una lunga gestazione – l'Italia adottò la prima legge in tema di reati informatici in recepimento della Raccomandazione del Consiglio d'Europa del 9 settembre 1989 n. R (89)-9[17].

Pur ricalcando esattamente la struttura dell'art. 640 c.p., la scelta del termine frode informatica in luogo del termine truffa costituisce il segno di una precisa valutazione legislativa. Ove si fosse trattato, infatti, di una ipotesi che si differenzia solo in riferimento al mezzo impiegato per perpetrare l'imbroglio, non ci sarebbe stato bisogno di introdurre una fattispecie autonoma. Sarebbe stato sufficiente, infatti, attrarre la casistica della truffa informatica nell'ambito di operatività dell'art. 640 c.p., così come avvenuto con le ipotesi – ad esempio – di truffa telefonica o, al massimo, prevedere una circostanza aggravante. La frode, invece, rinvia al concetto – magari meno tecnico – di inganno, ma sicuramente di più ampio respiro e proprio per questo idoneo a coprire una fenomenologia più vasta che non coincide con una categoria univoca[18].

D'altronde, l'opportunità del mancato allineamento terminologico trova la sua giustificazione anche nelle differenze tra gli elementi strutturali propri delle fattispecie. Nella truffa ordinaria è necessario rinvenire gli artifizi e i raggiri posti in essere consapevolmente dal soggetto agente, l'induzione in errore intesa come alterazione della rappresenta-

[17] È noto che all'epoca il legislatore italiano non ritenne la materia del *cybercrime* di rilevanza tale da giustificare l'introduzione di un titolo *ad hoc* all'interno del codice. Si preferì, piuttosto, rispettare il criterio dell'unità dell'oggetto giuridico, valorizzando le diverse tipologie di offesa nell'ambito di categorie di beni già individuati. Cfr. L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (diretto da), *Cybercrime*, cit., p. 35 ss.

[18] Lo stesso è avvenuto per le ipotesi di frode fiscale, frode assicurativa e frode bancaria, tutti casi non coincidenti con la truffa in senso stretto e per i quali il legislatore ha predisposto una disciplina specifica. Sul punto si veda E. Reccia, *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria*, in *Arch. Pen. Web*, 2022, 1; M. Borgobello, *La Cassazione sul rapporto tra accesso abusivo a sistema informatico, frode informatica e detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*, in *Giurisprudenza Penale Web*, 2020, 1; F. Vitale, *Brevi riflessioni sul reato di "frode informatica": i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cybercrime*, in *Arch. Pen.*, 2015, 1, p. 10.

zione mentale del soggetto passivo e, in ultimo, il danno patrimoniale diretto.

Diversamente, nella frode informatica vengono meno sia gli artifizi e i raggiri, poiché la condotta umana consapevole potrebbe ricoprire solo l'atto iniziale dell'inganno ma successivamente i cosiddetti *script* o *malware* agiscono in maniera automatizzata[19], sia l'induzione e lo stesso errore[20].

Il punto non è di poco conto e merita un approfondimento. Nel paradigma della truffa classica si assiste a una forma di cooperazione artificiosa, ove la volontà della vittima, da cui scaturisce un consenso viziato a causa dell'inganno, ha un ruolo attivo nella stessa lesione patrimoniale[21]. Nella frode informatica, invece, *l'atto di disposizione meccanico*[22] si sostituisce in concreto alla volontà umana e per questo motivo non è possibile considerarlo un mero strumento di reato[23], tanto più che la vittima potrebbe essere del tutto ignara dei meccanismi posti in atto[24].

[19] Così Cass. pen. Sez. II, sentenza 1 luglio 2020 n. 718, secondo cui «non sussiste evento intermedio dell'induzione in errore in frode informatica; le condotte di artifizi e raggiri sono sostituite da alterazione funzionamento sistema o intervento senza diritto su dati/programmi».

[20] Cass. pen. Sez. II, sentenza 05 febbraio 2020 n. 10354 osserva che la truffa e la frode informatica si differenziano «solamente perché l'attività fraudolenta dell'agente investe non la persona, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza di quest'ultima attraverso la sua manipolazione, onde, come la truffa, si consuma nel momento e nel luogo in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui».

[21] G. Fiandaca, E. Musco, *Diritto Penale*, cit., pp. 29 ss.

[22] L'espressione è di R. Bartoli, *La frode informatica tra «modellistica», diritto vigente, diritto vivente e prospettive di riforma*, in *Dir. Inf.* 2011, pp. 383 ss. Giova sottolineare che è pur sempre rinvenibile *ab origine* una condotta dolosa del reo alla base della manipolazione informatica, identificabile nel primo atto che spinge il sistema informatico a perpetrare l'imbroglio, tuttavia la frode in senso stretto è posta in essere dalla macchina.

[23] Cfr. Cass. pen. sez. III, sentenza 24 maggio 2012 n. 23798, conferma che il reato di frode informatica ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

[24] Si pensi, ad esempio, ai cd. *sevizi a valore aggiunto* (VAS), che sono spesso aggiunti via web a servizi di base in uso agli utenti a loro insaputa, attivati inconsapevolmente o fraudolentemente addebitati. In questi casi è evidente la mancanza dell'induzione in errore, essendo la vittima del tutto ignara e – dunque – mancando l'atto di disposizione volontario,

Non solo, ma la necessità di introdurre una fattispecie autonoma scaturisce anche dall'impossibilità di perpetrare un inganno ai danni di una macchina, motivo per cui tra gli elementi costitutivi dell'art. 640 *ter* c.p. manca appunto l'induzione in errore. Il sistema informatico, infatti, non è in grado di conoscere la realtà se non attraverso le operazioni di elaborazione dei dati che sono il risultato di istruzioni logiche predefinite. In altre parole, la macchina esegue un procedimento logico che corrisponde esattamente all'input (quand'anche falso o viziato), non essendo – così – riscontrabile alcun errore[25].

Infine, il danno sovente è diversificato rispetto all'ipotesi *ex* art. 640 c.p., potendo coincidere anche con la sottrazione di dati o con l'accesso non autorizzato, ipotesi entrambe non necessariamente suscettibili di una valutazione economica diretta. Questa eventualità si colloca tra quelle che concorrono alla smaterializzazione del concetto stesso di patrimonio di cui si è detto poc'anzi, estendendo quest'ultimo anche al *regolare funzionamento dei sistemi informatici*[26].

Non è questa la sede per ripercorrere approfonditamente i caratteri della frode informatica[27], volendo piuttosto concentrare l'analisi sul fenomeno del *cheating*, che si colloca a metà strada tra manipolazione psichica e abuso degli strumenti informatici, e la cui pervasività è tale da indurre a indagare la possibilità concreta di attrarlo nell'alveo proprio dell'art. 640 *ter* c.p.

In una prospettiva generale, per meglio comprendere il concetto di *cheating* si possono ripercorrere le riflessioni di Stuart Green in relazione ai casi rinvenibili nei crimini dei colletti bianchi[28], da cui se ne trae la

oltre alla totale meccanizzazione della frode, poiché il sistema preleva somma di denaro direttamente dal patrimonio del soggetto sulla base di una falsa informazione tecnica. Lo stesso schema è rinvenibile in molte altre ipotesi di *phishing*, sempre più sofisticate.

[25] Cfr. F. Vitale, *Brevi riflessioni*, cit., p. 1 ss. Si veda anche L. Picotti, *I contenuti penali della legge sull'intelligenza artificiale*, in *Sist. Pen*., 2025, p. 1 ss.

[26] Così F. Antolisei, *Manuale*, cit., p. 386.

[27] Per un'analisi della struttura della fattispecie di frode informatica, anche in un'ottica comparativista si veda C. Crescioli, *Cybercrime* e *tutela penale del patrimonio informatico*, Giuffrè, 2025, p. 156 ss.

[28] Così S.P. Green, *Lying, cheating, and stealing: a moral theory of white-collar crime*, Oxford University Press, 2006, p. 57 ss.

definizione: ‹‹the violation of a fair and fairly enforced rule with intent to gain an advantage over another with whom one is in a cooperative, rule-bound relationship››. Dunque, l'ipotesi si realizzerebbe quando il soggetto agente viene meno a un patto di correttezza vigente in un determinato contesto regolamentato, che – nel caso di specie – coinciderebbe con quello proprio dell'ecosistema digitale. In particolare, per aversi una ipotesi di *cheating* informatico è necessario riscontrare la violazione del complesso di regole intorno al quale si era creato il legittimo affidamento che tutti lo avrebbero rispettato e il conseguimento di un ingiusto vantaggio[29]. La rottura di quella che secondo la teoria dei giochi sarebbe la parità delle condizioni dei giocatori, dovuta al tradimento della fiducia nel rispetto dei codici posti alla base dei sistemi digitali, costituisce una grave violazione e genera un danno che va ben oltre quello del singolo e che si può riassumere nella perdita di credibilità, di valore economico e sociale dell'ecosistema[30].

Si è già avuto modo di affermare che *social engineering* e *cheating* si comportano come un Giano bifronte, in cui il primo fa leva sulla vulnerabilità del fattore umano per aprire la strada al secondo, diret-

[29] Green inquadra, sotto il profilo sistematico, le ipotesi di *cheating* tra i cosiddetti illeciti morali e distingue tre elementi costituitivi fondamentali: *culpability*, *social harmfulness* e *moral wrongfulness*. *Ibidem*, p. 58 ss.; si veda anche G. Virgo, *Cheating and Dishonesty*, in *The Cambridge Law Journal*, 2018, 77(1), p. 18 ss. Particolare allarme sociale destano le ipotesi di *cheating* accademico nei paesi di *common law*, ritenendosi che abbia raggiunto soglie importanti negli ultimi tempi. Cfr. L. Kennette - M. Jelenik, *Cheating: It depends how you define it*, in *Canadian Perspectives on Academic Integrity*, 2022, 5, 2, p. 16 ss.; D.L. McCabe - L.K. Trevino - K.D. Butterfield, *Cheating in Academic' Institutions: a Decade of Research*, in *Ethics & Behavior*, 2001, 3, p. 219 ss.

[30] La condotta di *cheating* genera un danno anche collettivo rilevante, nella misura in cui apre la strada a che tutti gli utenti ritengano conveniente barare e ha una diretta operatività in tutte le forme di *gaming*, soprattutto nel panorama degli sport elettronici (esport). Cfr. S. Gächter - F. Schulz, *Intrinsic Honesty and the Prevalence of Rule Violations across Societies*, in *Nature*, 2016, 531, p. 496 ss.; V.H. Hua Chen - Y. Wu - B. Wu, *A social-cognitive approach to online game cheating*, in *Computers in Human Behavior*, 2013, 29, p. 2557 ss. Sul tema degli esport si veda G. Bevilacqua - I. Infante, a cura di, *Framing legal and ethical issues in electronic sports from the perspective of International Law*, in *Il Nuovo Dir. Soc.*, 2025; A. Lepore - C. Di Carluccio - C. Ghionni, *Scenari giuridici degli e-sport in Italia nell'universo del gaming*, in *Il Nuovo Dir. Soc.*, 2025; G. Bevilacqua - A. Lepore, *Sport elettronici, sicurezza e diritti umani*, in *Quad. rass. dir. ec. sport*, 2024, 10.

to a violare i protocolli informatici; la sinergia tra le due tecniche dà luogo a un inganno tecnologico finalizzato a conseguire un indebito vantaggio. La differenza rispetto alle note forme di intrusione informatica (*hacking*) è all'apparenza sottile, ma in realtà molto rilevante: non si tratta di una manipolazione tecnica *tout court*, bensì di una vera e propria manipolazione psicologica che attiene alla vittima[31] e, solo in second'ordine, al sistema informatico.

Per quanto, allora, l'art. 640 *ter* c.p. si pone *prima facie* come il naturale punto di approdo dei casi di *cheating*, da un'attenta analisi degli elementi strutturali emerge una sussunzione solo apparente.

Per risolvere l'impasse è opportuno distinguere tre ipotesi.

La prima ha riguardo al *social engineering* puro, in cui la condotta del reo si risolve in una manipolazione della sfera psichica del soggetto passivo e, in tal caso, trova applicazione l'art. 640 c.p.

La seconda, invece, coincide con i casi in cui la condotta di *cheating* è assoluta, concretizzandosi in una manipolazione tecnica del sistema informatico a seguito della quale opera l'art. 640 *ter* c.p.

Infine, l'ultima è quella che presenta il maggior grado di complessità, riferendosi all'evenienza che entrambi i fenomeni convivano sovrapponendosi. Ricorrendo ai criteri dommatici propri del diritto penale, la coesistenza delle due fattispecie deve essere risolta ritenendo l'art. 640 *ter* c.p. speciale rispetto all'art. 640 c.p., in quanto – appunto – sostituisce l'elemento dell'induzione in errore che presuppone una vittima umana, con la manipolazione del sistema informatico.

Accade, quindi, che le tecniche di *social engineering* costituiscano solo un antefatto necessario del successivo *cheating*, come tale assorbito nella frode informatica. *A contrario*, se l'evento (ingiusto profitto/altrui danno) è conseguenza anche della condotta del soggetto passivo

[31] È noto che soprattutto nei casi di *phishing* si sfrutta la fiducia e il timore reverenziale che le persone hanno nei confronti di un'autorità o un'istituzione (fosse anche solo la propria banca) e che spinge le vittime a cedere le proprie informazioni o eseguire operazioni fraudolente. Stando ai dati forniti dall'*European Union Agency for Cybersecurity* (ENISA) nel documento *Threat Landscape 2025*, il phishing – principale tecnica di *social engineering* – rappresenta il 60% di tutte le forme di intrusione iniziale nei sistemi informatici, che nel nostro ordinamento danno luogo in larga parte a condotte di frode informatica, in *https://www.enisa.europa.eu/sites/default/files/20251/ENISA%20Threat%20Landscape%202025.pdf*.

a seguito dell'induzione in errore, allora troverà applicazione la truffa ordinaria.

Sin qui le ipotesi lineari, seppure complesse, che l'interprete è chiamato ad affrontare. Il problema è che la casistica offre scenari in cui non sempre risulta possibile distinguere i caratteri dell'una piuttosto che dell'altra ipotesi. Si consideri, ad esempio, il caso in cui il *cheater* si limita a sfruttare errori di programmazione preesistenti senza alterare il sistema informatico e ponendo in essere operazioni lecite (*glitch*), ovvero il caso in cui si fa ricorso a un *aimbot* per ottenere un vantaggio non di natura patrimoniale o, ancora, la situazione in cui si ottiene un risultato per il tramite di strumenti esterni che non alterano direttamente il *software*. Ebbene, in tutti questi casi la frode informatica non trova applicazione, mancando ora la condotta vincolata della manipolazione dell'apparato digitale, ora il danno patrimoniale diretto, se non addirittura l'ingiusto profitto.

Ci sono, poi, dei casi in cui la condotta di *cheating* è talmente sofisticata da sembrare lecita, come accade, ad esempio, nelle ipotesi in cui il soggetto agente si introduce nel sistema utilizzando credenziali corrette e legittimamente ottenute. In simili contesti la corrispondenza all'art. 640 *ter* c.p. sarebbe assicurata solo ove si riuscisse a dimostrare o l'inganno tramite il quale il reo è entrato in possesso delle chiavi di accesso corrette, o il cosiddetto *intervento senza diritto*, quando si utilizza il sistema per scopi diversi e incompatibili con quelli per cui l'accesso è stato concesso[32].

Anche in queste situazioni dirimente è la prevalenza del fattore umano rispetto al fattore tecnico, assumendo centrale rilevanza il destinatario dell'attività fraudolenta. Ove la condotta di *cheating* sia rivolta a indurre in errore una persona fisica, allora ricorrerebbero gli estremi della truffa ordinaria ai sensi dell'art. 640 c.p.; diversamente, se la frode ricade sul sistema informatico, troverebbe applicazione l'art. 640 *ter* c.p., fatta salva la possibilità di contestare altre fattispecie ove ne ricorrono i presupposti[33].

[32] In tal senso Cass. pen. Sez. Un., sentenza 27 ottobre 2011 n. 4694 e Cass. pen. Sez. Un., sentenza 18 maggi 2017 n. 41210. Più recentemente, Cass. Pen. Sez. V, sentenza 8 settembre 2022 n. 38152.

[33] In particolare, potrebbe trovare applicazione l'ipotesi prevista dall'art. 615 *ter* c.p. per i casi in cui si realizzi una condotta di accesso abusivo a un sistema informatico.

Le criticità poste dalle problematiche applicative riportano con forza in superficie il tema dell'ancoraggio dei reati contro il patrimonio alla dimensione materiale della cosa mobile. L'irrisolta questione rischia, infatti, di tradursi in un vuoto di tutela proprio in riferimento ai casi di *social engineering*. Si è detto che la prevalenza dell'elemento umano dovrebbe far ricadere tali ipotesi nel perimetro della truffa ordinaria, senonché l'operazione potrebbe trovare un ostacolo nella dematerializzazione dell'oggetto della tutela. Si pensi a un aspirante *trader* che per accreditarsi su una piattaforma di *trading online*, ricorre a tecniche di *social engineering* per convincere un soggetto esperto a cedergli le sue credenziali al solo fine di crearsi una reputazione digitale. Quest'ultima costituirebbe la *res digitalis* che come tale non configura un danno patrimoniale diretto per la vittima, determinando l'esclusione dell'operatività dell'art. 640 c.p. Al contempo, mancando la manipolazione tecnica del sistema informatico, non si configurerebbe neanche l'ipotesi disciplinata dall'art. 640 *ter* c.p., con la conseguenza che simili casi restano – *de iure condito* – impuniti.

A questo punto emergono due possibili suggerimenti. Da un lato, sarebbe opportuno cogliere l'occasione per un ripensamento del concetto di patrimonio alla luce della sua declinazione informatica, assicurando una tutela più ampia e maggiormente in linea con lo sviluppo tecnologico. Dall'altro, considerato l'ultimo rapporto dell'Agenzia dell'Unione Europea per la cybersicurezza (ENISA) in cui si sottolineano i rischi sempre maggiori delle condotte di *social engineering* e di *cheating* ritenute responsabili del 60% dei casi di frode informatica, si propone la revisione della figura prevista dall'art. 640 *ter* c.p. La nuova ipotesi di reato non dovrebbe essere ritagliata sulla falsariga della truffa classica, né trovarsi con essa in un rapporto di specialità. Dovrebbe, piuttosto, avere una struttura autonoma, atta a ricomprendere tutte le ipotesi di frode possibili, alla stregua di quanto già avvenuto nel Regno Unito con l'adozione del *Gambling Act* nel 2005[34]. In tale provvedimento il *cheating* costituisce proprio una fattispecie a sé, in cui la con-

[34] Il riferimento, *de iure condendo*, è alla struttura della condotta vietata, trattandosi di un provvedimento dedicato al settore specifico del gioco e delle scommesse. Cfr. *Gambling Act 2005*, Section 42, in *https://www.legislation.gov.uk/ukpga/2005/19/section/42.*

dotta vietata (sia attiva sia omissiva) coincide con l'atto di ingannare o interferire con il regolare svolgimento del gioco, a prescindere dal conseguimento di un effettivo vantaggio finanziario da parte del reo, ed elevando a bene giuridico tutelato (accanto all'integrità del sistema) il legittimo affidamento delle parti al rispetto delle regole.

Bisognerà indirizzarsi verso una simile soluzione, anche in considerazione del fatto che l'Italia ha firmato la Convenzione ONU contro la criminalità informatica del 2024, che adotta una visione unitaria della fattispecie di frode informatica, superando la dicotomia truffa-frode[35]. L'art. 13, infatti, raggruppa le ipotesi di furto e frode ai sistemi di informazione e comunicazione assoggettandole alla stessa disciplina e distinguendo tre modalità della condotta: l'intervento sui dati, l'interferenza sui sistemi e l'inganno tramite le tecnologie dell'informazione e della comunicazione (ICT) che induce la vittima a compiere ovvero omettere un atto. La disposizione richiede che sia ravvisabile l'intento fraudolento o disonesto di procurare a sé o a un terzo, senza diritto, un profitto in denaro o altri beni. Mentre la disciplina italiana opera una netta distinzione tra le due ipotesi facendo leva principalmente sul soggetto passivo (nella truffa la persona, nella frode il sistema informatico), la fattispecie di sintesi adottata dalla Convenzione ONU predilige, dunque, un approccio incentrato maggiormente sul mezzo impiegato per perpetrare l'offesa al fine di ricomprendere il maggior numero di condotte lesive possibili. Sembra questa la strada da seguire per affrontare un fenomeno criminoso la cui portata è sempre più evidente.

5. La progressiva consapevolezza da parte del legislatore della capacità offensiva delle condotte perpetrate nell'ecosistema digitale trova conferma anche nella previsione della circostanza aggravante al comma 2 dell'art. 640 *ter* c.p., che individua due diverse ipotesi.

La prima, introdotta contestualmente all'intervento del 1993, ha riguardo all'abuso della qualità di operatore del sistema nelle ipotesi

[35] Il 24 dicembre 2024 l'Assemblea Generale delle Nazioni Unite ha approvato la Convenzione sul *Cybercrime*, il primo Trattato sulla criminalità informatica dopo la Convenzione di Budapest del 2002. La Convenzione sarà aperta alla firma sino al 31 dicembre 2026, in *https://docs.un.org/en/A/79/460.*

in cui il soggetto agente – in virtù della sua qualifica che gli permette di accedere al sistema informatico – lede l'integrità dei sistemi digitali.

La seconda, invece, è stata disciplinata dalla legge 15 ottobre 2013 n. 119 ed è nota come furto di identità digitale[36]. La disposizione è rilevante non solo perché riconosce implicitamente valore giuridico all'identità digitale, ma soprattutto perché potrebbe costituire l'appiglio per il riconoscimento dell'autonomia del patrimonio informatico[37]. In tale ipotesi potrebbe rientrare anche il furto di identità digitale ad opera di un sistema di intelligenza artificiale, ma come regolamentare il caso in cui l'AI realizzi una simulazione di identità per ingannare la vittima o un altro sistema? Ove il *deepfake* si fondasse su dati biometrici sottratti a un soggetto terzo, non vi è dubbio che troverebbe applicazione l'aggravante citata. Cionondimeno, nel caso in cui l'AI ponga in essere un fatto di manipolazione psichica ricorrendo al *social engineering* dovrebbe applicarsi la fattispecie della truffa ordinaria[38]. Non prevedendo l'art. 640 c.p. un'aggravante corrispondente a quella contenuta nel co. 2 dell'art. 640 ter c.p., si creerebbe una sproporzione nel trattamento sanzionatorio[39]. Ancora una volta l'analisi porta a interrogarsi sull'opportunità di una regolamentazione specifica per i *cybercrime*.

Nell'era dell'intelligenza artificiale la possibilità che tali strumenti siano addestrati a ottenere ingiusti profitti per il tramite delle frode, costituisce un dato di realtà[40]. L'equivalenza tra manipolazione del sistema informatico e raggiro della vittima sul piano dell'offensività in concreto rinvia a un prossimo futuro in cui gli atti di disposizione patrimoniale

[36] Si tratta della legge 15 ottobre 2013 n. 119, recante *Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere*.

[37] Non è un caso che l'aggravante del furto di identità operi soprattutto nei casi di *phishing*. Cfr. G. Minicucci, *Le frodi informatiche*, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (diretto da), *Cybercrime*, cit., p. 827 ss.

[38] Si pensi al caso dell'intelligenza artificiale che clonando la voce del direttore di banca, induca in errore un impiegato, convincendolo a eseguire un bonifico non dovuto.

[39] L'art. 640 c.p. prevede la sanzione della reclusione da sei mesi a tre anni e la multa da euro 51 a euro 1.032, mentre per l'art. 640 *ter* co. 2 c.p. la pena va da due a sei anni e della multa da euro 600 a euro 3.000.

[40] Cfr. L. Picotti, *I contenuti penali della legge sull'intelligenza artificiale*, in *Sist. Pen.*, 2 dicembre 2025; C. Crescioli, *Cybercrime*, cit., pp. 32 ss.

potrebbero non essere sempre frutto della volontà umana. Questo desta un crescente e giustificato allarme sociale, soprattutto in considerazione del rischio di lesione dei diritti umani, quando le condotte fraudolente attaccano sistemi operanti in settori ad alta criticità.

Il riconoscimento diretto del patrimonio informatico alla stregua di un flusso informativo, allora, non si risolve in una mera questione tecnica, ma sarebbe la risposta all'esigenza da più parti avvertita di assicurare una tutela effettiva da forme di aggressione sempre più evolute.

Il superamento dell'elemento della materialità del patrimonio nella dimensione cibernetica costringe l'interprete anche a riconsiderare l'operatività di alcune categorie tradizionali, a cominciare dai criteri spazio-temporali[41], con particolare riferimento al *locus commissi delicti*, sottolineando ulteriormente la distanza tra la truffa classica e la frode informatica.

D'altronde, la dematerializzazione del patrimonio informatico è stata sancita anche nell'art. 2 della citata Convenzione ONU sul *Cybercrime* del 2024, secondo cui la nozione di 'beni' includerebbe tutte le risorse immateriali, quelle digitali e tutti gli strumenti legali che provano la titolarità di diritti su tali beni[42].

[41] Invero, per quanto concerne il momento consumativo, non si registrano sostanziali differenze tra le due ipotesi. Nella truffa tradizionale «il reato si consuma nel momento in cui si verifica l'ultimo degli eventi provocati dalla condotta ingannatrice, sia esso il danno o il profitto (ovvero nel momento in cui si verificano entrambi gli eventi, se realizzati in maniera simultanea)». Così G. Fiandaca - E. Musco, *Diritto penale*, cit. p. 201. Nella frode informatica il delitto si perfeziona nel momento è conseguito l'ingiusto profitto per il tramite della manipolazione informatica. Cfr. Cass. pen. Sez. II, sentenza 17 marzo 2020 n. 10354. Rispetto al luogo del reato, invece, l'ubiquità della rete e la distanza fisica tra i soggetti coinvolti, pone delle difficoltà. Per stabilire la competenza territoriale si dovrà guardare al luogo in cui è avvenuta parte dell'azione o omissione, così come previsto dall'art. 9 co. 1 c.p.p. o, in subordine, alla residenza, domicilio, dimora dell'imputato (co. 2). Cass, pen. Sez. II, sentenza 21 febbraio 2023 n. 10570 prende in considerazione o il luogo in cui si verifica l'alterazione del sistema, o il luogo in cui viene avvertito il danno. Cfr. anche Cass. pen. Sez. II, sentenza 23 aprile 2024 n. 34362, secondo cui il ricorso ai criteri suppletivi indicati deve seguire il tentativo di localizzare il profitto. Così anche Cass. pen. Sez. II, sentenza 15 luglio 2025 n. 25992.

[42] Il citato art. 2 così recita: ‹‹"Property" shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including virtual assets, and legal documents or instruments evidencing title to, or interest in, such assets››.

La transizione digitale impone, allora, una trasformazione del diritto penale da antropocentrico a tecnocentrico, senza che questo si traduca in una deumanizzazione del diritto. Tutt'altro, il riconoscimento delle specificità delle ipotesi strettamente connesse all'evoluzione tecnologica, non più mutuate dalla disciplina dettata per le fattispecie tradizionali, garantirebbe una tutela piena, effettiva ed efficace. Certo, per un rafforzamento del quadro giuridico è necessario implementare gli strumenti di prevenzione, con particolare riferimento a quelli previsti dalla normativa dell'Unione europea. Sia la Direttiva dettata in tema di *Network and Information Security* (NIS2)[43], sia il Regolamento *Cyber Security Act*[44], forniscono un'adeguata strategia sinergica: la prima impone protocolli di gestione del rischio atti a proteggere il patrimonio informatico, laddove il secondo certifica la qualità degli strumenti utilizzati tramite certificazioni europee.

[43] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), recepita in Italia con Decreto legislativo 4 settembre 2024 n. 138. In *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022L2555.*

[44] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»). E' in vigore dal 27 giugno 2019, si veda https://eur-lex.europa.eu/eli/reg/2019/881/oj/ita. Recentemente sono stati adottati due Regolamenti di esecuzione: il Regolamento di esecuzione (UE) 2024/3143 della Commissione e il Regolamento di esecuzione (UE) 2024/3144 della Commissione. In *https://eur-lex.europa.eu/eli/reg/2019/881/oj/ita.*

EU DIGITAL GOVERNANCE, DIGITAL IDENTITY, DATA AND FUNDAMENTAL RIGHTS

FROM REGULATION TO REALITY: HUMAN-RIGHTS IMPLICATIONS OF NATIONAL EU DIGITAL IDENTITY IMPLEMENTATIONS

Constanța Mătușescu

1. Digital identity constitutes a set of electronic characteristics and attributes that determine the identity of an individual within digital systems, integrating both objective elements of personality (legally recognised through official documents) and subjective elements (like personal and cultural affiliations)[1].

As digital technology today occupies a predominant place for the individual[2], digital identity increasingly determines access to services, opportunities and rights.

[1] See, *inter alia*, L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014; L. Vardanyan - O. Hamuk - H. Kocharyan, *Fragmented Identities: Legal Challenges of Digital Identity, Integrity, and Informational Self-Determination*, *European Studies*, 2024, vol. 11, n. 1 (September 2024), p. 105 ss.; G. Zaccaroni, *Fundamental rights and disruptive technologies: a right to personal identity under the European multi-level system of protection?*, in *Freedom, security & justice: European legal studies*, 2020, n. 3, p. 143 ss.; M. Robles-Carrillo, *Digital identity: an approach to its nature, concept, and functionalities*, in *International journal of law and information technology*, 2024, vol. 32, eaae019.

[2] According to a recent report, as of October 2025, there are 6.04 billion internet users worldwide, representing 73.2% of the global population, up over 5% by 2024 - Statista, *Number of internet and social media users worldwide as of October 2025 (in billions), https://www.statista.com/statistics/617136/digital-population-worldwide/*.

In cross-border contexts, digital identity plays a pivotal role as it enables the verification and authentication of individuals and entities beyond territorial boundaries, facilitating seamless interactions and transactions across nations. It functions as a core enabler in the digital economy by underpinning the trustworthiness and integrity necessary for digital commerce, government services, financial operations, and private sector engagements. Governments leverage digital identity systems to deliver efficient, secure, and accessible public services remotely, while private sectors utilize these identities to offer personalized and secure products, improve fraud detection, and enhance customer experiences.

Faced with this rapidly evolving reality, characterized by a growing overlap between physical and digital identities and a digital space increasingly dominated by private actors, concerns about ensuring the protection of digital identity are growing. These concerns have been accompanied by recognition of the need for multidisciplinary approaches that combine legal, technological, and policy perspectives to address the multifaceted nature of digital identity management[3], an approach centered on the user, reflected in the doctrine in the form of the concept of "self-sovereign identity"[4].

One of the most significant developments in this regard is that recorded at the level of the European Union (EU), which has undertaken an ambitious digital transformation agenda[5] and adopted a "European Declaration on Digital Rights and Principles"[6] which outlines a Euro-

[3] N. Purtova, *From knowing by name to targeting: The meaning of identification under the GDPR. International Data Privacy Law*, 2022, n. 12(3), p. 163 ss.

[4] A. Giannopoulou, *Digital identity infrastructures: A critical approach of self-sovereign identity,* in *Digital Society*, 2023, n. 2, p. 18.; S. Schwalm - I. Alamillo-Domingo, *Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0*, in *European Review of Digital Administration & Law - Erdal*, 2021, vol. 2, n. 2, p. 89 ss.

[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions *Shaping Europe's digital future*, COM/2020/67 final.

[6] European Parliament, Council, and the European Commission *European Declaration on Digital Rights and Principles for the Digital Decade,* 2023/C 23/01, PUB/2023/89, OJ C 23, 23.1.2023, p. 1 ss.

pean vision of human-centered digital transformation, the EU proposing that the digital transition respect fundamental rights, democracy and the rule of law, ensuring inclusion, accessibility and equality for all citizens.

In implementing this vision, the EU adopted, in April 2024, the European Digital Identity (EUDI) Regulation[7], by revising the 2014 Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) [8]. Its preamble states that everyone in the EU has the "right to a digital identity that is under their sole control and that enables them to exercise their rights in the digital environment and to participate in the digital economy." In order to establish a unified, secure, and interoperable digital identity system at EU level, Regulation (EU) 2024/1183 obliges all Member States to provide citizens, by the end of 2026, with *a European Digital Identity Wallet* (EDIW) capable of enabling cross-border authentication, verified credentials, and simplified access to both public and private services[9].

While the regulatory architecture is technologically advanced and normatively grounded in fundamental rights standards, the move from *regulation to reality* exposes, in addition to other problematic aspects (regarding, for example, the existing power imbalances between individuals and digital identity providers[10]), deep structural and societal disparities across Member States.

[7] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024 (sometimes referred to as eIDAS 2.0).

[8] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014.

[9] For an analysis of the functioning of this "EU's New Identity Model" see A. Kudra - A. Rieger - J. Sedlmeir - T. Roth - G. Fridgen - A. Young, *Digital Identity Wallets: A Guide to the EU's New Identity Model*, in *Information systems journal*, 2025, p. 1 ss.

[10] See S. Wong-Toropainen, *Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework*, in K. Prifti - E. Demir - J. Krämer - K. Heine - E. Stamhuis, *Digital Governance: Confronting the Challenges Posed by Artificial Intelligence*, T.M.C. Asser Press, 2024, p. 115 ss.

A central promise of the EUDI framework is *universal accessibility* - the idea that every person in the EU, regardless of socio-economic background, technological capacity, or physical ability, should be able to use the digital identity wallet on equal terms. However, the heterogeneity of national digital ecosystems raises serious concerns regarding the practical realisation of this principle[11]. The gap between highly digitalised states such as Estonia or Denmark and countries with persistent digital divides, such as Romania, creates a landscape in which the same European regulation may lead to vastly different human-rights outcomes.

Romania represents a particularly relevant case study because the country continues to face substantial challenges in terms of digital literacy, rural-urban infrastructural inequalities, and the lack of consistent accessibility measures for persons with disabilities and older adults. According to recent EU-wide assessments[12], Romania remains among the Member States with the lowest levels of basic digital skills and the highest proportion of citizens excluded from digital public services. Such structural constraints risk transforming the EUDI wallet - envisioned as a tool for empowerment and administrative simplification - into a mechanism that inadvertently *reinforces exclusion and discrimination*, especially for vulnerable groups.

Against this background, this article investigates the *human-rights implications of national EUDI implementations*, focusing specifically on the principles of accessibility, inclusion, and non-discrimination as articulated in the Charter of Fundamental Rights of the European Union and the broader European data-protection framework. By combining legal analysis with a comparative assessment of implementation strategies in several Member States, the article examines how Romania's national context may amplify or mitigate risks of digital exclusion.

[11] See M.E. Kjørven - K. Gjøsteen - T.L. Waerstad, *Safe and Inclusive or Unsafe and Discriminatory? European Digital Identity Wallets and the Challenges of 'Sole Control'*, 1 May 2025, available at SSRN: *https://ssrn.com/abstract=5238470.*

[12] Eurostat, *Skills for the digital age*, April 2024, in *https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Skills_for_the_digital_age.*

2. The regulatory architecture governing digital identity in the European Union combines a harmonized supranational framework with diverse national implementation models. Understanding this dual structure is essential for assessing the human-rights implications of national digital identity schemes, particularly as Member States operationalize the revised eIDAS framework and the new European Digital Identity Wallet (EUDI Wallet).

From an academic standpoint, the European legal framework reflects a longstanding normative commitment to trust, security, and cross-border digital harmonisation. Yet legal scholarship highlights an emerging tension between technological standardisation and the constitutional principles of proportionality, necessity, and user autonomy[13]. The practical realisation of these principles depends heavily on the institutional, infrastructural, and sociocultural context of each Member State.

The European legal framework for digital identity has developed progressively, strengthening a holistic approach that integrates electronic authentication, trust services and personal data protection.

The foundational instrument for digital identity governance in the EU is Regulation (EU) 910/2014 (eIDAS), the mandatory application of which began on 1 July 2016. It establishes rules for electronic identification, authentication, and trust services, aiming to secure cross-border recognition of national electronic identification (eID) schemes. eIDAS introduced a minimum set of assurance levels, obligations for Member States to notify national eID schemes, and rules for interoperability within the internal market. Its overarching objective is to enhance trust and security in electronic transactions while safeguarding users' rights, including privacy, data protection, and transparency[14].

[13] See G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022; L. Vardanyan - O. Hamuk - H. Kocharyan, *Fragmented Identities: Legal Challenges of Digital Identity, Integrity, and Informational Self-Determination*, *European Studies*, 2024, vol. 11, n. 1 (September 2024), p. 105 ss.

[14] S. Lips - N. Vinogradova - R. Krimmer - D. Draheim, *Re-Shaping the EU Digital Identity Framework*, in *Proceedings of the 23rd Annual International Conference on Digital Government Research 2022*, p. 13 ss.

In April 2024, the EU adopted Regulation (EU) 2024/1183, which significantly amends the 2014 eIDAS framework and lays the foundation for the European Digital Identity Wallet (EDIW/EUDI Wallet). This new regulation requires all Member States to provide citizens with a certified, secure, and user-controlled digital identity wallet by the end of 2026.

The development of this regulatory framework has been marked by a distinct movement from identity management as a sensitive area under national competence towards a harmonised and user-centric European digital framework, overlapping with the existing systems of the Member States[15]. This process reflects the recognition that in the digital age, cross-border interoperability and mutual recognition are essential for the functioning of the Digital Single Market and for the protection of citizens' fundamental rights.

The revised framework is grounded in principles emphasising: user control and autonomy (individuals must be able to determine which attributes are shared and under what conditions); data minimisation and privacy (only necessary data may be processed, and users must retain agency over their digital identity interactions); interoperability and standardisation (Member States must ensure that national systems interact seamlessly across borders and with the EUDI Wallet ecosystem); universal accessibility (the wallet must be designed to ensure inclusive and equitable access for all EU residents).

Read together with the *European Declaration on Digital Rights and Principles* (2022), the EUDI Regulation reflects the EU's commitment to a human-centric digital transformation that safeguards fundamental rights, democratic values, and equitable access to digital technologies.

The EU legal framework on digital identity is complemented by the Charter of Fundamental Rights of the European Union[16], the General Data Protection Regulation (GDPR)[17], and the Law Enforcement

[15] L. Weigl - A. Amard - C. Codagnone - G. Fridgen, *The EU's Digital Identity Policy: Tracing Policy Punctuations*, *International Conference on Theory and Practice of Electronic Governance*, 4-7 Oct., 2022, Guimarães, p. 74 ss.

[16] Charter of Fundamental Rights of the European Union, 2012 O.J. C 326/39.

[17] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data, OJ L 119, 4.5.2016.

Directive (LED)[18]. These instruments impose strict requirements concerning: lawfulness, fairness, and transparency of personal data processing; necessity and proportionality in the use of digital identity attributes; safeguards against surveillance, profiling, and misuse; user rights of access, rectification, erasure, and portability. Together, these norms establish the fundamental rights architecture within which EUDI Wallet implementations must operate.

The Court of Justice of the European Union (CJEU) has repeatedly stressed, in cases such as *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12)[19], that digital infrastructures must comply with the Charter of Fundamental Rights, particularly Articles 7 and 8 concerning privacy and data protection. *Digital Rights Ireland* predates eIDAS, but doctrinal interpretations emphasise its continued relevance for assessing proportionality in the processing of identity-related data. More recent scholarly commentary highlights the interplay between eIDAS and GDPR[20], particularly regarding lawful bases for processing identity attributes and the allocation of responsibilities between identity providers and "relying parties" (those companies and government agencies who want to access personal information from citizens' Wallets).[21]

Although litigation concerning the EUDI Wallet has not yet reached the CJEU, parallels may be drawn with jurisprudence on data minimisation and purpose limitation, such as *Schrems I* (C-362/14)[22] and

[18] Directive (EU) 2016/680 on the protection of personal data in the context of law enforcement, OJ L 119, 4.5.2016.

[19] Judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238).

[20] D. Baldini, *The Impact of the Right to Personal Data Protection on the Design of the European Digital Identity Wallet*, in *Italian journal of public law*, 2024, vol. 16, n. 1, p. 297 ss.; E. Podda - P. Hölzmer - A. Amard - J. Sedlmeir - G. Fridgen, *The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets*, in *Internet policy review*, 2025, vol. 14, n. 3, p. 1 ss.

[21] In this regard, see also *Open Letter to the European Commission from 15 Digital Rights and Consumer Organisations concerning privacy and transparency problems in the eIDAS Implementing Acts*, in *https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_iAs_OpenLetter_2025.pdf.*

[22] Judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650).

Schrems II[23] (C-311/18), which underscore the strict scrutiny applied to digital ecosystems processing sensitive personal data. The Wallet's architecture, involving verifiable credentials and cross-border interoperability, must therefore be interpreted in light of these precedents.

3. Each Member State of the European Union must adapt its national legislation to comply with the requirements set out in the eIDAS 2.0 Regulation and related European legal instruments. This adaptation involves not only the adoption of formal rules, but also the creation of the technical and institutional infrastructure necessary for effective implementation, including the establishment of competent bodies for the management of digital identity, the creation of interoperable digital platforms, the definition of identity verification and authentication procedures, and the implementation of safeguards for the protection of personal data[24].

The need for legislative harmonisation is not uniform, but takes into account the constitutional, cultural and legal particularities of each Member State. Some Member States already have advanced digital identity systems, with high degrees of public acceptance and integration into digital services. Others face challenges related to limited institutional capacity, insufficient investment in digital infrastructure and public reluctance towards digital identification systems, which leads to substantial practical implementation challenges. These disparities can lead to legal and technological fragmentation at European level, undermining the objectives of interoperability and the smooth functioning of digital markets.

Unlike the previous version of the eIDAS Regulation (EU/910/2014), based on the notification of national electronic identification schemes, the national implementation of the European Digital Identity (EUDI) introduced by Regulation (EU) 2024/1183 requires a

[23] Judgment of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, EU:C:2020:559).

[24] K. Degen - T. Teubner, *Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective*, in *Electronic markets*, 2024, vol. 34, n. 50, p. 49 ss.

harmonised approach, consisting of a common technical architecture, a reference framework and standards. Even though the European Digital Identity Wallets will be provided by the Member States and will be based on the national systems that already exist in some of them, this approach aims at the recognition and acceptance of digital identity solutions across the EU, promoting trust and interoperability. Large-scale pilot projects are currently testing the technical specifications for the common toolbox that will form the basis of the EDIW and the results are being considered when drawing up implementing acts[25].

Although this standardisation process is ongoing, a number of concerns have been expressed in academia and the profession about the extent to which it is possible to overcome the complex challenges arising from the interaction between existing digital infrastructures, the administrative capacity of Member States and the need to ensure compliance with European standards on fundamental rights, including accessibility, data protection and equal treatment. Some of these concerns concern the very way in which the European legal framework is constructed, which incorporates references to potential rights to digital access and a digital identity, which are mentioned in the Regulation but which lack formal and universal recognition as autonomous rights[26]. This legal gap raises fundamental questions about the status of these rights in national legal systems and how they can be protected and implemented *de facto*.

The shift from regulatory intent to national implementation demands more than technical optimization or compliance with technical specifications. It requires a *human-rights-by-design* approach that places fundamental rights at the center of digital identity governance from the earliest stages of system conception through ongoing operation and evaluation. This approach recognizes that digital identity systems are not neutral technical instruments but rather deeply political technologies that shape individual autonomy, collective agency, access to

[25] For a comprehensive overview of these developments, see the European Commission's EUDI page at *https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation*.

[26] A. Kaplane, *The European Digital Identity Wallet: A New Human Right Unlocked?*, in *Nordic journal of human rights*, 2025, vol. 43, n. 3, p. 304 ss.

essential services, and the distribution of power between citizens, corporations, and the state.

At the same time, data privacy remains a concern. Although the EUDI Regulation establishes a set of high-level requirements related to privacy and security, it does not explicitly specify the technologies that can be adopted in the development phase to meet these requirements. Research shows that inherent design choices maintain risks to user privacy, including linkability, identifiability, and excessive attribute data disclosure[27].

Privacy and data protection, enshrined in Article 8 of the European Convention on Human Rights and operationalized through the GDPR, must be actively protected through privacy-by-design principles embedded throughout identity system architecture, not treated as post-implementation compliance requirements.

Given the concerns across the Union about data breaches and increased surveillance, as well as people's reluctance to use biometric features, increasingly integrated into identity authentication systems due to their uniqueness and resistance to fraud, any breach in ensuring the strict standards set out in the GDPR (including necessity, proportionality and explicit consent of the user for the processing of biometric data) may significantly affect citizens' trust, undermining the adoption of the digital identity system based on such features.

Another major challenge identified in the doctrine and which has particular relevance in the context of this paper is related to the risk of discrimination and exclusion that the EUDI wallet presents. Such a risk derives, on the one hand, from the heterogeneity of national digital infrastructures. States such as Estonia, Denmark or Finland have mature, integrated digital ecosystems, with high levels of digital literacy, while other states – including Romania, Bulgaria or Greece – are faced with fragmented administrative digitalization and low levels of use of

[27] A. Sharif - M. Ranzi - R. Carbone - G. Sciarretta - F. A. Marino - S. Ranise, *The eIDAS regulation: A survey of technological trends for European electronic identity schemes. Applied Sciences*, 2022, vol. 12 (24), p. 1 ss.; A. Álvarez, P. Hölzmer, J. Sedlmeir, *Privacy evaluation of the European Digital Identity Wallet's Architecture and Reference Framework*, in *Computers & security*, 2026, n. 160, p. 1 ss.

electronic public services. This asymmetry generates the risk of a "two-speed implementation", in which states with advanced infrastructures quickly adopt the digital wallet, while others experience significant delays, reducing the uniformity of the benefits promised by the EUDI. This also affects the functioning of the internal market, as interoperability becomes effective only if all actors can operate with the same level of technological maturity.

On the other hand, certain socio-economic barriers and the lack of digital skills can fuel the risk of discrimination and exclusion. The implementation of EUDI assumes that users – regardless of age, income or geographical area – can access and use a digital wallet. In practice, however, there are major differences between urban and rural areas, low levels of digital literacy (especially among the elderly) and the minimum infrastructure (smart devices, stable internet connection) may be missing. In countries with structural deficits, EUDI can accentuate the digital divide, transforming a tool designed for inclusion into one that reproduces technological exclusion. For vulnerable people, the difficulty of using a digital wallet can amount to limiting access to essential services. Equality and non-discrimination demand that identity systems be designed to ensure equitable access across diverse demographic groups, with particular attention to protecting historically marginalized populations.

Informational self-determination – an emerging human right grounded in human dignity – requires that individuals retain meaningful control over their digital identity data and how it is disclosed to other parties.[28] This principle is particularly important in the EUDI context, as wallet systems fundamentally alter how personal information is collected, stored, and shared. According to the Regulation, the digital identity, which allows access to public and private services online and offline throughout the Union, is under the "exclusive control" of the user, who thus has the possibility «to request, obtain, select, combine, store, delete, share and securely present ... personally identifiable

[28] F. Thouvenin, *Informational Self-Determination: A Convincing Rationale for Data Protection Law?*, in *Journal of intellectual property, information technology and electronic commerce law (JIPITEC)*, 2021, vol. 12, n. 4, p. 246 ss.

data»[29]. The doctrine notes that this control «is often out of reach for individuals with limited digital skills, disabilities, or those who rely on third-party assistance. Others may fall victim to fraud, coercion, or social engineering attacks»[30]. Thus, including in highly digitized countries, such as the Scandinavian ones, the strict interpretation of this requirement has already resulted in significant digital exclusion for vulnerable groups, and its transformation by the Member States, in the process of implementing the EUDI, into a rigid legal obligation (in the form of a prohibition on providing access credentials to a third party), could have important consequences both in terms of accessibility and liability.

Accessibility and universal design principles must be embedded into all aspects of EUDI implementation to ensure that systems do not inadvertently exclude persons with disabilities or others facing accessibility barriers[31].

4. To understand how EU principles can be put into practice, it is useful to analyze the states that are already at the forefront of digitalization.

Estonia's digital identity system[32] is among the world's most advanced, providing citizens with secure digital identification for accessing public and private services. Since 2001, every citizen has received a digital identity at birth, used for almost any administrative task, from online voting to accessing medical records[33]. The e-ID ecosystem includes se-

[29] Article 5a 4. (a) of Regulation (EU) 2024/1183.

[30] M. E. Kjørven - K. Gjøsteen - T. L. Waerstad, *Safe and Inclusive or Unsafe and Discriminatory? European Digital Identity Wallets and the Challenges of 'sole control'. Computer Law & Security Review*, 2025, n. 60, p. 1 ss.

[31] Relevant in this regard is Directive (EU) 2019/882 (JO L 151, 7.6.2019), which entered into force on 28 June 2025 and imposes new accessibility requirements for products and services, including information systems and electronic communications equipment. While the EEA addresses accessibility of the product (e.g., the Wallet interface), it does not fully cover the entire ecosystem of access (e.g., digital literacy, in-person support for onboarding, and structural factors). The legal mandate for the EUDI Wallet must be designed to mitigate systemic exclusion, not just technical inaccessibility.

[32] *https://e-estonia.com/solutions/estonian-e-identity/id-card/.*

[33] T. Martens, *Electronic identity management in Estonia between market and state governance*. *Identity in the Information Society,* IDIS, 2010, vol. 2, n. 1, p. 213 ss.

cure digital ID cards, mobile ID, and smart ID applications, to which is added, since 2014, e-Residency, a unique program allowing non-residents to access Estonian e-services and build borderless businesses [34].

The foundation of this system is the X-Road infrastructure, a decentralized platform considered as a leading model of Digital Public Infrastructure (DPI) worldwide that ensures interoperability between various databases, while maintaining security and transparency. Estonia has implemented a data tracker which allows citizens clear access to an overview of operations being performed with their data. It's designed to interface with public sector information systems that store and process their personal data. The "once-only" principle prevents requiring the same information multiple times. The system supports digital signatures with legal equivalence to handwritten signatures. Approximately 99% of government services are available online, saving an estimated 2% of GDP annually in efficiency. At the same time, it is estimated that by using a digital signature each citizen saves an average of five working days annually.

The Estonian model demonstrates that a digital identity system can work effectively on a national scale and certain components of it can even attract a global audience, as in the case of the e-Residency program. This mature model has actively shaped the EU eIDAS regulation and integration with EDIW is expected to be relatively smooth.

Estonia's success is based on a long-term strategy aimed at improving the state's competitiveness and increasing the general well-being of its inhabitants, with the public sector as a leader in pursuing the principles of information society development, on investments in infrastructure and, crucially, on building public trust through transparency and robust security.

However, even in Estonia, challenges related to the digital divide persist, especially among the elderly population and in rural areas[35].

[34] P. Tammpuu - A. Masso, *Transnational digital identity as an instrument for global digital citizenship: The case of Estonia's E-residency*, in *Information systems frontiers,* 2019, vol. 21, p. 621 ss.

[35] A. Leppiman - I. Riivits - Arkonsuo - A. Pohjola, *Old-Age Digital Exclusion as a Policy Challenge in Estonia and Finland*, in K. Walsh - T. Scharf - S. Van Regenmortel - A. Wanka, (eds) *Social Exclusion in Later Life*. *International Perspectives on Aging*, 2021, vol. 28, Springer, Cham; K. Leetmaa - M. Bochkova - K. Kangro - T. Kübar - K.L. Lepik - I.

Denmark has followed a similar approach[36], adopting a digitalization strategy with clear, regularly updated objectives more than two decades ago, focusing on creating an accessible and user-friendly digital ecosystem.

The Danish e-government system is recognized for its efficiency, and the country is among the European leaders in the adoption of digital technologies. Characterized by a secure national digital infrastructure that includes the digital key MitID[37] and the official communication channel Digital Post[38], Denmark has one of the highest levels of digital service usage in the European Union.

The transition from the previous infrastructure (NemID, a form of two-factor authentication in which residents used a key card to verify their identity, introduced in 2010) to MitID (launched in 2022 to improve usability and enhanced security) was managed through a broad information and support campaign, providing assistance to citizens who encountered difficulties, including through local service centers and dedicated telephone lines. This model emphasizes the importance of leaving no one behind, recognizing that not all citizens have the same level of digital skills. Investments in digital education and infrastructure[39] have contributed to high adoption rates and reduced social inequalities.

Pastak - B. Plüschke - Altof, *Digital transformation through the lens of peripheralisation: Double exclusion of ageing rural localities in an advanced e-country. European Urban and Regional Studies*, 2025.

[36] L.S. Yuliantini - E.P. Purnomo, *The Comparative Analysis of E-Government Development in Denmark and Estonia*, in *Journal of Government and Politics*, March 1, 2024; A. Scupola, *A Case Study of Digital Transformation of Danish Public Services: Actors and Policies*, in I. Williams edited by, *11th CMI International Conference, 2018: Prospects and Challenges Towards Developing a Digital Economy within the EU* (p. 14 ss.). Article 8624818 IEEE Press.

[37] *https://www.mitid.dk/en-gb/.*

[38] *https://en.digst.dk/systems/digital-post/.*

[39] A. Scupola - I. Mergel, *Co-production in digital transformation of public administration and public value creation: The case of Denmark, Government Information Quarterly*, 2022, vol. 39, n. 1, p. 1 ss.

5.1. Unlike the mature systems existing in states such as Estonia or Denmark, tested for several decades, digital identity measures in Romania practically began in the context of the implementation of EU Regulation 910/2014 (eIDAS) and have only recently intensified, with the European Digital Decade Policy Programme 2030, established by Decision (EU) 2022/2481, which required the adoption, in October 2024, of the National Action Plan for the Digital Decade for Romania 2030[40], a strategic document that aims to align national action directions with European values and targets. A recent assessment finds that "the roadmap has numerous shortcomings in terms of ambition, coherence, governance, monitoring and accountability mechanisms, as well as its credibility when assessed against the objectives of the EU Digital Decade"[41]. Among the problematic aspects, it is highlighted that Romania has not yet defined 2030 objectives for digital identity.

Although that Romania's legal ecosystem remains reactive rather than anticipatory in matters related to digital transformation, some progress has been made. Thus, Romania has notified its national electronic identification scheme - ROeID - under Article 9 of eIDAS. This notification signifies that the system meets the technical and security conditions for mutual recognition across the EU, integrating Romania into the broader European identity infrastructure. ROeID provides the authentication layer for public-sector and private-sector digital services and is designed to interoperate with future EUDI Wallet requirements.

National implementation advanced through the introduction of the *Electronic Identity Card (CEI)*, regulated by Government Ordinance No. 12/2023[42]. The CEI includes a secure chip enabling electronic authentication, digital signature capabilities, and integration with na-

[40] *https://www.adr.gov.ro/autoritatea-pentru-digitalizarea-romaniei-anunta-aprobarea-oficiala-a-planului-national-de-actiune-privind-deceniul-digital-pentru-romania/.*

[41] Romanian Center of European Policies (CRPE), Report Romania's Digital Decade 2030 Roadmap: Building coherence, collaboration, and accountability, 29 October 2025, in *https://www.crpe.ro/wp-content/uploads/2025/10/CRPE-Romanias-Digital-Decade-2030-Roadmap-Building-coherence-collaboration-and-accountability.pdf.*

[42] Government of Romania, Ordinance no. 12 of January 31, 2023 amending and supplementing certain normative acts containing provisions regarding the registration of persons and the electronic identity card (Official Gazette no. 84 of January 31, 2023).

tional eID services. From 2025 onward, CEI issuance has expanded progressively across Romanian counties following initial pilot phases.

The CEI serves as a primary credential for accessing digital public services, aligning Romania with the obligations of the eIDAS framework and the future EUDI Wallet ecosystem. Its legal basis sets technical, security, and procedural rules regarding issuance, revocation, biometric data processing, and interoperability[43].

Romania's broader digital identity ecosystem is supported by legislation governing electronic signatures, trust services, cybersecurity, and data protection. Together with the CEI regulatory framework and ROeID scheme, these instruments form the national legal architecture through which eIDAS and eIDAS 2.0 obligations are operationalized.

Through the Romanian Digitalization Authority (ADR), it is actively involved in the European Wallet Consortium (EWC) pilot project and participates in testing use cases, such as storing travel credentials and organizing payments.

Despite a relatively consolidated legal framework, Romania faces a complex set of challenges in implementing the EUDI Wallet, which reflects deeper structural gaps. Although there is political will to accelerate digitalization, especially in the post-pandemic context and through the National Recovery and Resilience Plan (PNRR), the reality on the ground is marked by significant discrepancies[44]. In the assessments carried out at the European Union level[45], Romania, ranked last in many of the digitalization indicators, is one of the countries slowing down the march towards the 2030 targets.

[43] Romania National Identity Card Portal, in *https://carteadeidentitate.gov.ro.*

[44] For a recent assessment, see Digital Nation, *Digital Governance Framework for Romania*, October 2025 (*https://edgeinstitute.ro/wp-content/uploads/2025/10/Digital-Governance-Framework-for-Romania-by-Digital-Nation.pdf*), which provides a clear radiograph of the existing situation: «Critical enablers such as eID, once-only and digital-first principles, digital signature's equivalence to the handwritten one, and data exchange between agencies all exist in principle. In practice, however, they are either underused or confined within single institutions. The core problem is clear: there is no customer-centric, whole-of-government perspective, no clear accountability for driving it, and no delivery capability to make it real. In short, Romania suffers from a vacuum in strategic digital governance».

[45] See the Commission reports on the state of development of the digital decade at *https://digital-strategy.ec.europa.eu/ro/library/state-digital-decade-2025-report.*

5.2.1. Romania's digital infrastructure landscape reveals significant disparities between urban and rural areas, with important implications for EUDI implementation. While urban centers, particularly Bucharest and major cities, have developed relatively advanced digital infrastructure supporting robust broadband connectivity and smartphone penetration, rural regions face substantial connectivity challenges (especially regarding 5G coverage)[46]. According to the recent State of the Digital Decade 2025 report, although it leads the EU in high-speed internet, rural areas, especially sparsely populated ones, still face limited access to high-speed internet, and in some regions coverage is below the EU average for high-speed connectivity (VHCN - Very High Capacity Networks). This infrastructure disparity creates the foundation for potential digital exclusion; citizens without reliable internet connectivity cannot effectively use mobile-based EUDI wallets, effectively excluding them from services increasingly dependent on digital identity verification.

The infrastructure barriers extend beyond simple connectivity to encompass the reliability, affordability, and accessibility of digital services themselves. Many rural communities lack not only broadband infrastructure but also the technical support services and training opportunities available in urban areas. When technical problems arise - compatibility issues with older devices, authentication failures, account lockouts - rural users often lack convenient access to customer support or technical assistance. This creates a cascading effect where infrastructure barriers combine with support service gaps to produce complex exclusion.

5.2.2. Beyond infrastructure, Romania faces significant challenges related to digital literacy and skills development, particularly among specific demographic groups[47]. According to the Digital Decade 2025

[46] According to the National Institute of Statistics, in 2024, 88.6% of homes will have internet access (fixed or mobile), but the urban area will have a higher percentage (92.5%). Although the gap has narrowed, 30% of rural areas do not benefit from high-speed internet, in *https://insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2024.pdf*.

[47] Făgăraș Research Institute, *Digital inclusion and exclusion in Romania 2022: a national study*, 01.12.2022, in *https://icf-fri.org/digital-inclusion-and-exclusion-in-romania-2022-a-national-study/*.

Report, only 27.7% of Romania's population has basic digital skills, well below the EU average of 55.6% and slightly below Romania's 2023 result of 27.8%.

While younger, urban populations generally demonstrate higher levels of digital competence, older adults, rural residents, and those with limited formal education often lack the digital skills necessary to confidently navigate complex systems like EUDI wallets. Research on digital literacy in healthcare contexts - where digital transformation has proceeded rapidly - reveals that healthcare professionals and patients alike frequently lack adequate understanding of complex digital systems, creating barriers to meaningful engagement[48].

The relationship between digital literacy and age is particularly pronounced; longitudinal research demonstrates that older adults experience significantly higher rates of digital exclusion, associated with lower digital skills and reduced motivation to adopt new technologies[49]. When digital identity systems become mandatory or strongly incentivized for accessing essential services, older adults disproportionately face barriers to access.

5.2.3. Romania's e-government infrastructure remains fragmented across multiple platforms, agencies, and regulatory frameworks[50]. Rather than a unified national identity infrastructure supporting seamless cross-agency credential recognition and service delivery, Romanian e-government consists of parallel systems with limited interoperability. This fragmentation creates several problems relevant to EUDI implementation. First, it suggests that integration of EUDI into existing e-government services will require substantial technical and regulatory coordination work. Second, it indicates that existing e-government systems may not embody best practices in accessibility or inclusive design, meaning EUDI implementation should not simply replicate existing

[48] I.M. Păcuraru - A. Năstac - A. Zamfir - S. Busnatu - O. Andronic - A.R. Artamonov, *Digital Transformation of Medical Services in Romania: Does the Healthcare System Meet the Current Needs of Patients?*, in *Healthcare*, 2025, n. 13, p. 1 ss.

[49] A. Dobre, *Decalajul digital și excluziunea digitală a vârstnicilor în România - un studiu de caz în București-Ilfov*, *Calitatea Vieții*, 2022, XXXIII, n. 4, p. 264 ss.

[50] OECD, *Digital Government Review of Romania: Towards a Digitally Mature Government,* OECD Digital Government Studies, OECD Publishing, 2023.

patterns. Third, the fragmented landscape suggests institutional capacity gaps that may impede rapid, effective EUDI deployment.

The experience, although recent, of the introduction of the CEI, reflects an undesirable way in which these problems can have an impact on the confidence of citizens and, ultimately, on the adoption rate of the digital wallet. Thus, despite the remarkable progress of the CEI project, reflected by the figure of over half a million documents already issued at national level, the institutional reality betrays a worrying gap between the pace of adoption by citizens and the effective capacity of institutions to capitalize on these tools, with numerous public authorities continuing to operate without the minimum equipment with CEI readers and without clear procedures for integrating them into workflows. The lack of logistical preparation and staff training, corroborated with the absence of a unitary implementation strategy, may lead to a scenario in which the digital wallet becomes devoid of content, discrediting the very architecture of electronic identity. This is especially true given that public trust in Romanian institutions is low, with a high level of distrust in the Parliament, Government and Presidency. At the same time, trust in the security of digital systems is affected by the perception that the state's digitalization is slow and by the risks of cybersecurity incidents. Romanians want more efficient digital public services, without bureaucracy, where the real stakes are trust in the fairness and efficiency of the systems[51].

It is therefore clear that without a national digital education campaign and strong guarantees on the protection of personal data, the adoption of the EUDI wallet could be extremely low. The experience of other countries shows that success does not only depend on technology, but also on building a culture of trust and digital competence.

In April 2025, far behind other states, the implementation of the National Interoperability Platform began[52], which will allow public

[51] See the Study conducted by Edge Institute & AtlasIntel on Romanians' perceptions of digital transformation, November 2025. *https://www.caleaeuropeana.ro/studiu-ritmul-digitalizarii-statului-considerat-lent-de-84-dintre-romani-eliminarea-drumurilor-la-ghisee-dorinta-nationala/.*

[52] *https://www.adr.gov.ro/anunt-de-inceput-de-proiect-platforma-nationala-de-interoperabilitate-pni-cod-smis-333977/.*

and private entities to exchange data in a secure and standardized environment, allowing the implementation of the "once only" principle. A solid operationalization of the Platform could lead to overcoming the problems previously reported.

Another critical point remains the lack of human resources in digital administration, the lack of ICT specialists in public institutions being mainly caused by uncompetitive salaries. Independent studies show that there are many civil servants who do not use ICT in their duties and public servants' digital skills remain low, despite being a focus of the NRRP[53].

Implementing EUDI requires cybersecurity expertise, certification authorities, and standardisation bodies. Chronic underfunding and limited institutional capacity may push Romania to rely excessively on private intermediaries, potentially raising concerns about accountability, vendor lock-in, and rights-compliance.

6. The combined EU and national frameworks shape the real-world conditions under which digital identity systems may either strengthen or undermine fundamental rights. European doctrine increasingly frames digital identity as a "constitutional infrastructure," necessitating robust safeguards against exclusion, surveillance, and asymmetric power relationships[54].

The European Union's eIDAS 2.0 Regulation, which entered into force in May 2024, represents a transformative shift in digital governance across the EU. By obliging Member States to provide their citizens with the European Digital Identity Wallet (EUDI Wallet) by 2026, this regulation establishes a new paradigm for how citizens interact with both public and private digital services. The EUDI Wallet aims to solve critical challenges by providing a unified, portable, and secure digital identity platform that prioritizes user sovereignty over their personal data. This vision promises enhanced accessibility to services,

[53] Digital Nation, *Digital Governance Framework for Romania*, October 2025, cit.

[54] G. De Gregorio - R. Radu, *Digital constitutionalism in the new era of Internet governance,* in *International journal of law and information technology*, 2022, vol. 30, n. 1, p. 68 s.

reduced bureaucratic friction, and greater citizen control over digital credentials.

However, the translation from European regulatory intent to national implementation reveals significant complexities. While the eIDAS 2.0 framework emphasizes self-sovereign identity principles and user empowerment, its successful deployment depends critically on how individual Member States - each with distinct institutional histories, technological infrastructures, and socioeconomic conditions - adapt these principles to their specific contexts. Romania, as an EU member state with particular demographic, infrastructural, and regulatory characteristics, exemplifies both the opportunities and challenges inherent in this localization process.

The implementation of the European Digital Identity Wallet represents a huge opportunity for the modernization and efficiency of society, objectives assumed but whose achievement is much delayed, compared to other states. However, for this transition to be fair and to respect human rights, it is imperative that Member States, including Romania, adopt a proactive and citizen-centered approach.

From a human rights perspective, the Romanian state has positive obligations to ensure effective and non-discriminatory access to digital services. This involves not only technical infrastructure, but also digital literacy programs, accessible interfaces for people with visual or mobility impairments, as well as maintaining alternative authentication channels for those who cannot use the digital wallet. The EUDI Regulation explicitly allows for the existence of equivalent non-digital mechanisms, but the transposition of these guarantees at national level must be clearly provided for by legislation and a dedicated budget. Another important risk is indirect discrimination: apparently neutral criteria, such as the obligation to use a mobile application, can have disproportionate effects on certain groups. In this regard, the implementation of the EUDI must respect the principle of proportionality and include Human Rights Impact Assessments (HRIA), not just data protection DPIAs.

Concrete policy recommendations flowing from this analysis include: (1) establishing explicit accessibility and inclusion requirements

in national EUDI implementation legislation, going beyond EU minimums to address Romania-specific barriers; (2) investing substantially in digital infrastructure development, particularly in rural areas, and ensuring affordable access; (3) implementing comprehensive digital literacy and training programs targeting vulnerable populations; (4) creating robust complaints and remedy mechanisms enabling affected persons to challenge discriminatory practices; (5) establishing participatory governance structures ensuring meaningful involvement of civil society and affected communities in EUDI system design and deployment; and (6) maintaining non-digital pathways and support services for essential identity verification, refusing to allow EUDI to become a complete substitute for traditional identification documents and services.

In conclusion, accessibility and inclusion cannot be treated as secondary elements of digital identity but are prerequisites for the respect of fundamental rights. The implementation of EUDI in Romania must be based on a "human rights by design" approach, which integrates social and ethical considerations from the technical and legislative design phase.

LA CYBERSECURITY E IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI: PROFILI DI INTEGRAZIONE E COORDINAMENTO

Antonio Vertuccio

1. L'evoluzione digitale ha fatto sorgere molteplici profili di criticità per la tutela dei diritti fondamentali degli individui.

Tra le istanze di salvaguardia emerse nell'ambiente digitale figura la sicurezza, o meglio, la cybersecurity[1], essenziale per assicurare la fruizione dei diritti nel cyberspace[2] e di preminente importanza nelle contemporanee dinamiche belliche.

[1] Per un inquadramento dei profili giuridici che vengono in rilievo nel cyberspace si rimanda a: AA.VV., *Global cybersecurity and international law*, in A. S. Serrano (a cura di), Routledge, 2024; R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in *La sicurezza nel cyberspazio*, in R. Ursi (a cura di), Franco Angeli, 2023, p. 7 ss.

[2] Alla luce dell'evoluzione normativa e dottrinale è possibile affermare che il cyberspace sia: «una realtà fisica e virtuale che estende e talvolta sfida le norme e i confini del solo spazio fisico, creando una nuova economia, nuove relazioni sociali, nuove dinamiche di potere e nuove minacce per le nostre vite». La definizione in questione è stata delineata da: E. Longo, *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in *La Regolazione europea della società digitale*, in F. Pizzetti (a cura di), Giappichelli, 2024, p. 206. Il riferimento fatto alla cybersecurity, quale condizione per il godimento di taluni diritti ha a oggetto la protezione dei dati personali, il diritto alla libertà di espressione, che può essere compromesso da attacchi cyber, atti a dar luogo a illegittime censure, interferenze o manipolazioni, il diritto alla sicurezza e il diritto all'informazione, violato da operazioni cibernetiche in grado di limitare la fruibilità di informazioni nel cyberspace, fonte principale per l'informazione nell'attuale contesto sociale.

Sul piano internazionalistico, gli esperti di diritto internazionale hanno redatto il Manuale di Tallin[3], attraverso il quale hanno affermato che "la scala e gli effetti" delle operazioni cibernetiche assumono una valenza dirimente per verificare se l'attacco cyber possa essere qualificato come uso della forza, o, nel peggiore dei casi come attacco armato.

Il contenuto della richiamata fonte di *soft law* è indicativo della prioritaria valenza della cybersecurity per la protezione della sicurezza nazionale.

Al contempo, la resilienza delle infrastrutture digitali è una preliminare condizione, che deve sussistere per evitare violazioni del diritto alla protezione dei dati personali.

Segnatamente, la sicurezza del trattamento è uno degli obblighi, che il *General Data Protection Regulation* (GDPR)[4] impone ai titolari del trattamento (cui successivamente si farà riferimento).

Invero, il presente contributo mira a soffermarsi su questo secondo fronte d'indagine, funzionale ad approfondire i profili di correlazione esistenti tra cybersecurity e diritto alla protezione dei dati personali.

Per perseguire questa finalità si analizzeranno le fonti emanate per promuovere la cybersecurity nel contesto europeo e talune disposizioni del GDPR.

La suddetta ricostruzione normativa consentirà di verificare in che modo sia stata promossa la sicurezza nel cyberspace e permetterà di comprendere come alcune norme in tema di cybersecurity possano de-

[3] La prima versione del Manuale di Tallin è stata adottata nel 2013, mentre la seconda versione nel 2017. I Manuli sono stati redatti da esperti di diritto internazionale con il supporto organizzativo del NATO Cooperative Cyber Defence Centre of Excellence a Tallin. In quest' ottica, emerge l'efficacia generativa della soft-law. I cyber-attacks, infatti, sono ormai uno strumento in grado di causare gravi conseguenze sul normale svolgimento della vita degli individui, causando disordini e fragilità nel contesto sociale. Sul punto e sull'applicazione del diritto internazionale ai cyber-attacks si rimanda a: S. Shackelford, *Analyzing the rise of nation – state sponsored ransomware attacks and their impact on insurance markets*, in *Global cybersecurity and international law*, in A.S. Serrano (a cura di), Routledge, 2024, p. 127 ss.

[4] Parlamento europeo e Consiglio dell'Unione europea, Regolamento 2016/679, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati*, Bruxelles, 2016.

finire, o meglio, specificare il contenuto di talune prescrizioni, contenute nel GDPR, che mirano a proteggere i dati personali.

2. Per approfondire la correlazione esistente tra cybersecurity e protezione dei dati personali appare necessario ricostruire la rapida e rilevante evoluzione del quadro normativo europeo circa la sicurezza informatica[5].

In questa prospettiva, è opportuno fare un preliminare riferimento alla direttiva 90/387/CEE[6] sull'istituzione del mercato interno per i servizi delle telecomunicazioni, la quale evidenziava come fosse necessario sviluppare la trasparenza, la parità di accesso e la sicurezza in rete.

La direttiva in questione rappresenta la base normativa della politica europea in materia di tecnologia e servizi per la società dell'informazione.

Successivamente, le istituzioni europee hanno promosso la cybersecurity nel contesto europeo attraverso la direttiva *Network and Information Security* (NIS)[7], la cui base giuridica era l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE)[8].

Ebbene, la cybersecurity veniva identificata come un presupposto per alimentare lo sviluppo del mercato unico interno.

Infatti, la medesima era funzionale a garantire la continuità dei servizi digitali, necessaria per la libera circolazione di beni e servizi nell'ambiente digitale in una prospettiva prevalentemente economica.

[5] Per una ricostruzione dell'approccio europeo alla cybersecurity si rimanda a: R. A. Wessel, *Towards EU cybersecurity law: Regulating a new policy field*, in *Research Handbook on International Law and Cyberspace*, in N. Tsaugourias - R. Buchan (a cura di), Edwar Elgar, 2015, p. 403 ss.

[6] Parlamento europeo e Consiglio dell'Unione europea, Direttiva 90/387/CEE, *sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni*, Bruxelles, 1990. La direttiva è stata poi abrogata dalla direttiva 2002/21/CE.

[7] Parlamento europeo e Consiglio dell'Unione europea, Direttiva 2016/1148, *recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione*, Bruxelles, 2016.

[8] L' articolo 114 TFUE attribuisce alle istituzioni europee il potere di adottare misure di armonizzazione, volte al riavvicinamento delle disposizioni legislative, regolamentari e amministrative.

Al contempo, però, come in parte anticipato in sede introduttiva, la cybersecurity oggi ha assunto una dimensione valoriale differente, strettamente interconnessa alla salvaguardia della sicurezza nazionale e alla tutela dei diritti fondamentali.

In questi termini, dunque, è rilevabile un'evoluzione in merito alla funzionalizzazione della cybersecurity, testimoniata dai diversi e più incisivi approcci normativi, che si sono registrati in seguito.

La suddetta direttiva, successivamente abrogata, prevedeva degli obblighi in capo agli Stati membri, estrinsecazione dell'acquisita consapevolezza circa l'esigenza di affermare il concetto di sicurezza nel cyberspazio.

Nello specifico, imponeva agli Stati membri di dotarsi di una strategia nazionale in materia cyber, istituire e partecipare a un gruppo di cooperazione al fine di agevolare lo scambio di conoscenze tra gli Stati membri, nonché la creazione di un gruppo di intervento per la sicurezza informatica in caso di incidenti.

La normativa si contraddistingueva per l'imposizione di diversi obblighi di sicurezza (attraverso l'intermediazione degli Stati membri) e notifica in capo agli operatori di servizi essenziali e fornitori dei servizi digitali.

In particolare, gli operatori di servizi essenziali erano identificati nelle entità in grado di fornire un servizio essenziale per il mantenimento di attività sociali/economiche critiche.

La sussunzione nel novero degli operatori essenziali dipendeva anche dall'eventualità che un incidente sui sistemi, utilizzati per la fornitura del servizio, avrebbe avuto effetti significativi sulla continuità del servizio.

La direttiva attribuiva agli Stati membri il potere di identificare gli operatori dei servizi essenziali nell'ambito dei settori elencati dall'Allegato II della stessa[9].

In quest'ottica, gli Stati membri, una volta individuati gli operatori di servizi essenziali, dovevano far sì che quest'ultimi e i fornitori di

[9] Mentre, i fornitori di servizi digitali venivano identificati in specifici settori quali quello marketplace online, motori di ricerca online e servizi di cloud computing.

servizi digitali adottassero misure appropriate per prevenire e ridurre al minimo l'impatto degli incidenti sulla sicurezza della rete[10].

La predetta fonte mirava a dar luogo a una minima armonizzazione in termini di cybersecurity, ma aveva generato talune divergenze di ricezione all'interno dei singoli Stati membri.

Infatti, l'ampia discrezionalità riconosciuta agli Stati membri nell'identificazione dei destinatari degli obblighi e nella relativa attuazione aveva causato una frammentazione del mercato interno e potenziali effetti pregiudizievoli sul suo funzionamento, con ripercussioni sulla fornitura transfrontaliera di servizi e sul livello di cyber - resilienza generale.

Dette divergenze avevano dato luogo a una maggiore vulnerabilità di taluni Stati membri di fronte alle minacce informatiche, con potenziali ricadute sull'intera Unione.

Per queste regioni è stata emanata la direttiva NIS 2[11], caratterizzata dall'identificazione di nuovi destinatari degli obblighi ivi sanciti.

In particolare, è applicabile anche alla pubblica amministrazione e a soggetti pubblici e privati, che operano in settori strategici come quello dell'energia, dei trasporti, qualificabili come medie imprese, che svolgano la loro attività all'interno dell'Unione.

La normativa opera una distinzione tra soggetti essenziali e importanti, facendo rientrare nel primo gruppo le pubbliche amministrazioni e gli operatori del settore energetico, spaziale, mentre tra i soggetti importanti sono annoverati gli operatori di servizi postali, del settore agroalimentare e di gestione dei rifiuti[12].

[10] Gli Stati membri dovevano garantire che le misure di sicurezza tenessero conto della sicurezza dei sistemi e delle infrastrutture, della gestione degli incidenti e della sussistenza di un'attività di monitoraggio continuo.

[11] Parlamento europeo e Consiglio dell'Unione europea, Direttiva 2022/2555, *relativa a misure per un livello comune elevato di cibersicurezza nell'Unione*, Bruxelles, 2022.

[12] Dall'applicazione sono esclusi i soggetti operanti in settori come la sicurezza nazionale, la difesa e l'attività di perseguimento dei reati. Al di là della qualificazione di media impresa, la direttiva si applica ai soggetti che forniscano reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico, siano prestatori di servizi di fiducia o registrino dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio.

Fatta questa precisazione, sul piano contenutistico la direttiva dispone che gli Stati membri provvedano affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete, che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi. Inoltre, la suddetta prescrizione mira a prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Nel valutare la proporzionalità di tali misure, la direttiva dispone che gli Stati debbano tenere conto del grado di esposizione dei soggetti a rischio, della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

Le menzionate misure sono basate su un approccio multirischio, che implica una definizione delle politiche di analisi dei rischi e di sicurezza dei sistemi informatici, una gestione e una continuità operativa, una sicurezza della catena di approvvigionamento, strategie per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza, autenticazioni a più fattori e sicurezza delle risorse umane.

Le suddette misure sistemiche sono indicative del cambio di paradigma normativo, basato sull'evoluzione del concetto di cybersecurity, inteso non più come mera protezione tecnica dei sistemi informatici, ma come processo proattivo di gestione del rischio.

Il suddetto processo proattivo è caratterizzato da una valutazione del rischio continua e dinamica e dall'integrazione della cybersecurity nei processi decisionali e di governance dei soggetti tenuti a osservare la direttiva.

Tale centralità della cybersecurity sul piano decisionale è desumibile dall'imposizione di una gestione e di una continuità operativa, che implica una definizione a monte di una strategia efficace in tema di cybersecurity, ma anche dall'articolo 20 della direttiva, che mira a responsabilizzare gli organi di gestione dei soggetti.

Inoltre, alla luce di tale prescrizione, i soggetti essenziali e importanti sono tenuti ad adottare una valutazione anticipata dei rischi esterni all'organizzazione, derivanti da partner strategici e fornitori (come *cloud provider* e fornitori IT, facenti parte della catena di approvvigionamento).

Segnatamente, l'approccio multirischio, connotato dall'enucleazione delle descritte misure, assume una fondamentale rilevanza per delineare standard di sicurezza efficaci nel cyberspace.

Al contempo, la fonte europea in questione si distingue sicuramente per la restrizione della discrezionalità degli Stati in merito all'individuazione dei soggetti destinatari delle relative prescrizioni e dal relativo ampliamento.

In seguito, le istituzioni europee hanno emanato un Regolamento, il *Cyber Resilience Act*[13], volto a sanare i perduranti profili di criticità inerenti alla sicurezza nell'ambiente digitale.

Il Regolamento si contraddistingue per un chiaro mutamento di paradigma normativo, in quanto, in una prospettiva orizzontale, identifica gli attori privati come i destinatari immediati delle prescrizioni ivi contenute.

Il suddetto approccio orizzontale risulta essere particolarmente apprezzabile, in virtù del fatto che mira a prevenire le possibili vulnerabilità dei sistemi digitali attraverso degli obblighi, vigenti già nella fase di fabbricazione dei medesimi.

Il Regolamento promuove la valorizzazione della cybersecurity, quale presupposto necessario per salvaguardare non solo il mercato interno, ma anche la sicurezza, la democrazia e la salute[14].

Nei Considerando del Regolamento viene anche rilevata l'assenza di un quadro normativo orizzontale dell'Unione, che stabilisca requisiti di cybersicurezza completi per tutti i prodotti con elementi digitali.

In tal senso, assume valenza centrale nel Regolamento la definizione di prodotti con elementi digitali, identificabili in qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remo-

[13] Parlamento europeo e Consiglio dell'Unione europea, Regolamento 2024/2847, *sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali*, Bruxelles, 2024. Sulla direttiva si rimanda a: F. Bavetta, *Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo*, in *Media., Riv. dir. med.*, 2023, p. 405 ss. Sul rapporto tra Direttiva NIS 2 e Cyber Act si rimanda a: P. Eckhardt - A. Kotovskaia, *The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive*, in *International Cybersecurity Law Review*, 2023, p. 147 ss.

[14] In questi termini ritorna la rilevanza della cybersecurity in svariati contesti come quello bellico.

to, compresi i componenti software o hardware immessi sul mercato separatamente.

In relazione a tali prodotti vengono stabilite una serie di prescrizioni in tema di cybersecurity.

In primo luogo, i prodotti con elementi digitali possono essere immessi sul mercato solo se soddisfano i requisiti di cybersicurezza delineati nel Regolamento. Inoltre, il Regolamento medesimo fa riferimento anche alla diversa categoria dei prodotti con elementi digitali importanti[15], i quali sono soggetti alle procedure di una particolare valutazione della conformità, da effettuare, in realtà, in forme diverse, per tutti i prodotti con elementi digitali.

I destinatari degli obblighi in tema di cybersecurity sono i fabbricanti dei prodotti con elementi digitali[16], tenuti a mettere a disposizione sul mercato i prodotti in assenza di vulnerabilità note, a garantire la fruibilità di aggiornamenti per far fronte a sopraggiunte vulnerabilità e a proteggere gli utenti da accessi non autorizzati mediante meccanismi di controllo.

Da queste disposizioni emerge come il Regolamento imponga degli obblighi direttamente operanti sugli attori privati, tenuti a promuovere una sorta di *security by design* su un piano parallelo alla *privacy by design*[17], di cui al Regolamento europeo per la protezione dei dati personali.

[15] I prodotti con elementi digitali importanti presentano rischi più elevati per la sicurezza informatica o possono dar luogo a un rischio significativo di effetti dannosi.

[16] Definiti dal Regolamento come: «Una persona fisica o giuridica che sviluppa o fabbrica prodotti con elementi digitali o che fa progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializza con il proprio nome o marchio, a titolo oneroso, di monetizzazione o gratuito».

[17] In merito al principio di privacy by design si rimanda a: EUROPEAN DATA PROTECTION BOARD (EPDB), *Orientamenti 4/2019 sull'articolo 25 protezione dei dati fin dalla progettazione e per impostazione predefinita*, 2020, disponibile su: epdb.europa.eu.

L'Organismo europeo indipendente ha evidenziato che il titolare del trattamento dovrebbe scegliere opzioni e impostazioni per il trattamento dei dati, tali da garantire che venga effettuato solo se il trattamento sia strettamente necessario per conseguire la specifica e lecita finalità. Inoltre, il titolare è tenuto a definire in anticipo per quali finalità specifiche, esplicite e legittime i dati personali vengano raccolti e trattati. Le misure devono essere adeguate a garantire che siano trattati solo i dati necessari per ogni specifica finalità del trattamento. Alla luce di questa enucleazione giuridica l'EPDB ha delineato i principi di trasparenza, correttezza, liceità, esattezza, minimizzazione e integrità cui i titolari del trattamento devono attenersi per tendere verso un'attuazione della *privacy by design.*

Si ritiene che il suddetto approccio orizzontale possa essere efficace per pervenire a elevati standard di cybersecurity, basati sull'anzidetta *security by design*, in grado di rafforzare l'etica della resilienza delle infrastrutture digitali fin dalla loro fabbricazione.

Inoltre, parte degli obblighi incombenti sui fabbricanti permette di cogliere la correlazione tra cybersecurity e protezione dei dati personali, oggetto d'esame più avanti.

Infatti, il Regolamento dispone che i prodotti con elementi digitali debbono proteggere la riservatezza e l'integrità dei dati personali e trattare solo i dati necessari a perseguire la finalità prevista. Medesimi obblighi gravano anche sugli importatori[18], qualora precedentemente i fabbricanti abbiano ottemperato ai loro obblighi.

Da ultimo, nel caso in cui venga sfruttata un'eventuale vulnerabilità del prodotto, il fabbricante è tenuto a effettuare una notifica al *Computer Security Incident Response Team* (CISRT) e *all'European Union Agency for Cybersecurity* (ENISA), volta a dare conto della vulnerabilità riscontrata, del soggetto che l'ha sfruttata e dei tipi di rimedi operabili[19].

Inquadrate le fonti, tese a configurare un quadro armonioso in materia di cybersecurity nel contesto europeo, appare necessario soffermarsi sulla correlazione tra normative in tema di cybersecurity e protezione dei dati personali.

3. Dall'analisi delle fonti riportate (nello specifico il *Cyber Act*) emerge come sia necessario indagare sulla correlazione esistente tra cybersecurity e protezione dei dati personali.

Invero, il diritto alla protezione dei dati personali nel corso degli ultimi decenni è stato particolarmente esposto a violazioni nell'ambiente digitale. Le prescrizioni contenute nel GDPR, volte a stabilire che la cessione dei dati personali possa avvenire in presenza di un consenso

[18] Definiti dal Regolamento come: «Una persona fisica o giuridica stabilita nell'Unione che immette sul mercato un prodotto con elementi digitali recante il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione».

[19] I fabbricanti sono anche tenuti ad esercitare la dovuta diligenza, allorquando integrano nei prodotti elementi provenienti da soggetti terzi per evitare che venga compromessa la cybersicurezza del prodotto.

informato, esplicito e libero degli individui[20] sono state sostanzialmente disattese nell' ecosistema digitale[21]. In particolare, le varie sanzioni[22], comminate dai garanti nazionali agli attori privati, evidenziano come le importanti norme contenute nel GDPR, pietra miliare per la protezione dei dati personali dal carattere a – territoriale[23], siano state inosservate in modo perdurante. L'opacità funzionale, che ha connotato l'ambiente digitale, ha portato al mancato rispetto dell'articolo 22 del GDPR, il quale dispone che l'interessato abbia diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, che produca effetti giuridici che lo riguardino. Infatti, l'acquisizione dei dati personali da parte degli attori privati è stata prodromica alla profilazione[24] e al successivo *microtargeting* (in ambito politico, ad esempio per condizionare le elezioni politiche, o commer-

[20] EDPB, *Guidelines 5/2020 on consent under Regulation 2016/679*, 2020. Queste linee guida vanno a integrare il parere 15/2011 del gruppo di lavoro articolo 29, istituito dalla direttiva 95/46/CE, costituito da un gruppo di esperti indipendenti e sostituito dall'EDPB, disponibili al sito: *https://www.edpb.europa.eu.*

[21] Lo status quo dell'ambiente digitale è testimoniato anche da una recente ricerca accademica, che ha dimostrato come circa il 50 per cento di siti web presi in analisi acquisisca dati personali anche in assenza del consenso degli interessati, attraverso un opaco funzionamento dei *cookie*, sul punto: A. Rasaii - H. Dao - A. Feldmann - M. Javid - O. Gasser - D. Gosain, *Intractable Cookie Crumbs: UNveiling the Nexus of Stateful Banner Interaction and Tracking Cookies*, in *arXIv*, 2025.

[22] Tra le altre si riportano le seguenti sanzioni: CPO Magazine, *France Issues £ 325 Milion GDPR Fine to Google for Sneaky Cookie*s, 2025, disponibile su cpomagazine.com; Commission Nationale de l'Informatique et des Libertès (CNIL), *Cookies: CNIL fined Yahoo £10 milion, 2024*, disponibile su: *https//www.cnil.it*; Noyb.eu, *Belgian DPA settlement turned into proper leagl orders on deceptive cookie banner*s, 2024, disponibile su: *https//noyb.eu.it.*

[23] EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR*, 2018. La versione adatta dopo le pubbliche consultazioni risale al 12 novembre 2019, disponibili al sito: *https://www.edpb.europa.eu.*

[24] Definita dal GDPR come: «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

ciale)[25], che si sostanzia nella trasmissione di contenuti pubblicitari *ad hoc*, idonei a produrre effetti giuridici sugli utenti, in assenza di un consenso realmente informato circa le finalità del trattamento[26]. La sintetica ricostruzione operata induce a rilevare importanti criticità circa la protezione dei dati personali degli individui. Nel contesto così delineato, indicativo del crescente potere assunto dagli attori privati come le piattaforme digitali, è opportuno soffermarsi sui profili dialettici tra cybersecurity e protezione dei dati personali[27].

Nello specifico, si ritiene che a tal fine debba essere analizzato l'articolo 32 del GDPR.

Questa disposizione statuisce che il titolare[28] e il responsabile del trattamento[29] debbano mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

Le misure in questione sono rappresentate dalla pseudonimizzazione (tecnica con la quale i dati personali non vengono resi direttamente attribuibili all'interessato), la capacità di assicurare su base permanente la riservatezza, l'integrità e la resilienza dei sistemi e servizi di trattamento, la capacità di ripristinare l'accesso ai dati personali e una pro-

[25] Sul tema si rimanda a: M. Bianca, *La filter bubble e il problema dell'identità digitale*, in *Media., Riv. dir. med.*, 2019, p. 39 ss. In ambito politico, recentemente, la Corte costituzionale rumena ha annullato il risultato delle elezioni parlamentari del 2024, in quanto condizionate da una campagna di disinformazione attraverso il social network *Tik Tok*, per un approfondimento si rimanda a: O. Pollicino, *Se la disinformazione condiziona i processi democratici*, in *Il Sole 24 ore*, 2025.

[26] Le linee guida sul processo decisionale automatizzato fanno espressamente rientrare tra gli "effetti giuridici" la capacità della decisione (o, meglio, l'incidenza del contenuto trasmesso), basata sul trattamento automatizzato, di incidere sul voto nel contesto di un'elezione.

[27] Per un approfondimento sui profili ontologici di questa correlazione si rimanda a: B. Ponti, *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in *Riv. Ital. di Inform. e Dir.*, 2024, p. 57 ss.; F. Resta, *Cybersicurezza e protezione dati: un rapporto ambivalente*, in *Riv. Ital. di Inform. e Dir.*, 2024, p. 67 s; E. Sorrentino - A.F. Spagnuolo, *Cybersecurity e sovranità digitale nella promozione dei dati personali*, in *Riv. Ital. di Inform. e Dir.*, 2024, p. 685 ss.

[28] Persona fisica o giuridica, autorità pubblica, servizio o organismo che decide finalità e mezzi del trattamento dei dati personali.

[29] Persona fisica o giuridica che tratta i dati personali per conto del titolare del trattamento.

cedura per verificare l'efficacia delle misure adottate per garantire la sicurezza del trattamento. Questa disposizione fa esplicito riferimento alla sicurezza del trattamento, implicitamente correlabile al concetto di cybersecurity.

Ebbene, si ritiene che il contenuto della medesima possa essere specificato, o meglio, enucleato dalle disposizioni in tema di cybersecurity, contenute nel *Cyber Resilience Act*.

In special modo, le norme contenute nel Regolamento (nello specifico quelle contenute nell'allegato I) potrebbero fungere da parametro di riferimento per verificare l'efficacia delle misure, adottate dal titolare del trattamento per garantirne la sicurezza.

Segnatamente, la trasposizione, in realtà già in *re ipsa*, di queste norme nel precipuo ambito della protezione dei dati personali sarebbe possibile in virtù dell'ampiezza della definizione di prodotti con elementi digitali, contenuta nel Regolamento in tema di cybersecurity, e del riferimento nell'articolo 32 GDPR all'integrità e resilienza dei "sistemi e servizi di trattamento".

Infatti, si ritiene che i concetti di sistema e servizio del trattamento possano essere sussunti nel novero dei "prodotti con elementi digitali".

In virtù della suddetta trasposizione, basata sull' allegato I del Regolamento, si potrebbe ritenere che il titolare del trattamento debba garantire che il trattamento non sia connotato da vulnerabilità sfruttabili note e l'eventuale insorgenza delle stesse possa essere affrontata mediante aggiornamenti di sicurezza.

Inoltre, dovrebbe garantire la protezione dall'accesso non autorizzato mediante meccanismi di controllo come sistemi di autenticazione e gestione dell'identità o dell'accesso.

Al contempo, la compenetrazione tra l'allegato I del Regolamento in tema di cybersecurity e l'articolo 32 del GDPR è testimoniata dalla lettera e dello stesso allegato, che, come visto antecedentemente, fa riferimento all'obbligo di salvaguardare la riservatezza dei dati personali.

In questa diversa prospettiva, all'estremo opposto della correlazione, la tutela dei dati personali diventa parte integrante della cybersecurity, assumendo le vesti di un ineludibile presupposto per ottemperare al Regolamento e rendere i prodotti con elementi digitali sicuri.

In questi termini, nella lettera e dell'allegato I è possibile scorgere il tentativo di riaffermare il principio di *privacy by design*, sostanzialmente violato nell'ambiente digitale.

Quindi, in considerazione di quanto evidenziato, è possibile ritenere che il *Cyber Resilience Act* contenga disposizioni in grado di rafforzare il diritto alla protezione dei dati personali.

Altresì, la lettera e dell'Allegato è forse la più rilevante ai fini dell'estrinsecazione del contenuto prescrittivo dell'articolo 32 del GDPR. Infatti, dispone che la protezione della riservatezza dei dati personali debba essere assicurata criptando i pertinenti dati a riposo o in transito mediante meccanismi all'avanguardia.

In sostanza, il Regolamento in tema di cybersecurity intensifica la protezione dei dati personali sia *ex ante,* nella fase di progettazione dei prodotti con elementi digitali, che *ex post,* stabilendo degli standard di tutela di sicurezza, capaci di sviluppare le prescrizioni di cui all'articolo 32 del GDPR.

Ciò induce a ritenere che queste disposizioni, di cui all'Allegato I, possano divenire parametro per valutare l'eventuale responsabilità del titolare del trattamento (ed eventualmente del responsabile) per non aver adottato misure adeguate ad assicurare la sicurezza del trattamento.

In altri termini, si potrebbe ritenere che le suddette previsioni normative possano divenire un criterio di responsabilità per valutare se lo sforzo diligente del titolare del trattamento sia sufficiente per ottemperare all'articolo 32 del GDPR.

Le misure previste dall'Allegato I del Regolamento potrebbero essere un criterio di determinazione della "prestazione", cui è tenuto il titolare del trattamento in forza dell'articolo 32 del GDPR, delimitando il perimetro dello sforzo diligente richiesto al medesimo titolare per evitare di incorrere in responsabilità personali per la mancata osservanza dell'articolo 32 del GDPR.

4. La cybersecurity ha assunto una valenza centrale nel contemporaneo contesto digitale. L'assenza di stringenti normative, tese a promuovere la cybersecurity nel contesto europeo, ha indotto le istituzioni europee a delineare una disciplina tesa a implementarne la sicurezza in rete.

Fonti come la direttiva NIS 2 e il *Cyber Resilience Act* rappresentano un importante passo in avanti per la definizione di armoniosi standard di cybersecurity all'interno degli Stati membri.

L'evoluzione normativa in materia è indicativa di come sia sempre più necessaria un'applicazione orizzontale delle prescrizioni normative.

L'imposizione di efficaci standard di cybersecurity è uno dei presupposti necessari per garantire la protezione dei dati personali.

Infatti, la resilienza delle infrastrutture digitali è essenziale per assicurare che i dati personali contenuti nei prodotti digitali siano inaccessibili da fonti terze.

Invero, la cybersicurezza è una precondizione, che deve sussistere affinché il trattamento dei dati personali sia conforme al GDPR, e, quindi, lecito.

In questi termini, l'allegato I del Cyber Act potrebbe delimitare il perimetro prescrittivo dell'articolo 32 del GDPR e divenire il parametro di riferimento per verificare se il titolare del trattamento abbia profuso uno sforzo diligente e adeguato per scongiurare i rischi, che possono venire in rilievo per la sicurezza del trattamento.

Tale delimitazione potrebbe consentire di eliminare le zone grigie di responsabilità dei titolari del trattamento, dando luogo a un innalzamento degli standard di sicurezza del trattamento medesimo.

La correlazione in questione dimostra come l'efficace promozione della cybersecurity a livello normativo sia prodromica a un'implementazione della salvaguardia del diritto alla protezione dei dati personali nel contesto digitale, rispondente a logiche private, foriere di ataviche criticità circa la definizione di standard di tutela elevati.

Dunque, in continuità con le premesse introduttive, appare ancor più evidente e tangibile che la cybersecurity sia un preminente presupposto da garantire per assicurare e sviluppare la tutela del diritto alla protezione dei dati personali nell'ecosistema digitale.

Le suddette riflessioni corroborano la necessità, sempre più percettibile, di adottare un approccio interdisciplinare alle questioni critiche inerenti alla protezione dei dati personali, prodromico a implementare la tutela della sfera personale degli individui.

SICUREZZA E TRASFERIMENTO DATI EU-US: FOCUS SUL DATA PRIVACY FRAMEWORK

Valentina Barela

1. La migrazione al digitale ha dato inizio ad una nuova era di sviluppo economico e sociale nella quale il processo di digitalizzazione dei dati rappresenta un elemento catalizzatore. La generazione e trasmissione continua di dati[1], non sempre compiute attraverso azioni consapevoli degli utenti, mostrano implicazioni di diversa natura che riguardano una moltitudine di diritti e dinamiche economiche che non coinvolgono solo il diritto alla privacy e i diritti in generale della personalità, ma anche il diritto dell'antitrust[2], posto che l'adeguato utilizzo

[1] Per una prima classificazione di "dati" si v. j. Sylvestre Bergé - S. Grumbach - V. Zeno-Zencovich, *The "Datasphere", Data Flows beyond control, and Challenges for Lw and Governance*, in *European Journal of Comparative Law and Governance*, 2018, vol. 5, n. 2, p. 149.

[2] Per un'analisi sui rischi di abusi di posizione dominante e pratiche collusive nell'era dei Big data, nonché sul ruolo svolto dall'Autorità Garante Antitrust si v. G. Muscolo, *Big data e concorrenza: Quale rapporto?*, in *Informazione e Big Data tra innovazione e mercato*, a cura di V. Falce - G. Ghidini - G. Olivieri, Giuffrè, 2017, p. 173 e ss.; G. Pitruzzella, *Big data, Competition and Privacy: a look from the antitrust perspective*, in *Concorrenza e mercato*, fasc. 1, 2016, p. 15. In merito ad una prospettiva di analisi alla luce del Digit Market Act si veda C. Carli, *Accesso ai dati tra Gdpr, tutela concorrenza e Dma: un gioco di specchi?*, in *Mercato, concorrenza, regole*, 2022, p. 660.

dei big data è il presupposto per la libera concorrenza e quindi il corretto funzionamento di un mercato mondiale.

È indiscutibilmente riconosciuto che l'ubiquità e l'importanza economico-sociale del trattamento dei dati[3], anche in ragione dell'utilizzo dei dati per i processi di profilazione che registrano esigenze e preferenze degli utenti, favorisce la efficienza operativa, l'innovazione e la crescita economica di ogni sorta di attività, da quelle governative, economico finanziarie, a quelle personali[4].

I dati sono diventati una risorsa economica chiave per le imprese e significativo ed elevato è il rischio che si sviluppi un'economia di dati, monopolizzata dalle grandi imprese, a discapito delle altre più piccole e più deboli, coinvolgendo in tal modo non solo i diritti della persona ma anche i diritti strettamente economici, con rilevanti ripercussioni sul mercato, anche in termini di concorrenza sleale[5], sebbene gli stessi diritti fondamentali, nelle diverse declinazioni, trovano attuazione anche attraverso la tutela della sicurezza e della concorrenza, garante quest'ultima anche del benessere del consumatore finale[6]. La natura

[3] Così C. Kuner, *Protecting EU Data outside EU borders under the GDPR*, in *Common Market Law Review* 60:77-106, 2023, ed in particolare a p. 79.

[4] Sull'enucleazione dei "dati" quali oggetto principale dell'attività commerciale si v. G. G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transazionale dei dati personali*, in Dir. *inf.,* 2025, p. 909; A. Stazi - F. Corrado, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inf.*, n. 2, 2019, p. 442; A. Addante, *La circolazione negoziale dei dati personali nei contratti di fornitura e di contenuto e servizi digitali*, in *Gius. civ.*, n. 4, 2020, p. 889.

[5] Non di rado acquisizioni di imprese sono motivate dalla quantità di dati di cui è in possesso l'impresa acquisita o incorporata ed è evidente che il controllo dati che l'impresa risultante dalla concentrazione può alterare la concorrenza in ragione degli "effetti collaterali". Così si v. M. Maggiolino, *I big data tra Stati Uniti e Unione Europea*, in *Informazione e big data tra innovazione e concorrenza*, cit., p. 267.

[6] La convergenza tra la materia antitrust e il diritto alla privacy non è tuttavia sempre diffusamente recepita. Difatti, negli US, su cui ci si soffermerà a seguire (in merito al rapporto trasferimento dati europei), le corti statunitensi si mostrano più indulgenti della Commissione europea non riscontrando che ipotesi di concentrazioni di dati possano riflettere negativamente sulla tutela della privacy e sulle scelte dei consumatori (come nei casi Facebook /WhatsApp, Microsoft/LinkedIn, Google/DoubleClick). Tuttavia, parte della dottrina statunitense coglie la necessità di una convergenza, così M.E. Stucke - A.P.

globale delle attività commerciali comporta che le organizzazioni, nelle loro diverse vesti, necessitino di trasferire un insieme di dati personali alle società appartenenti al gruppo[7], esterne alla giurisdizione statale e accentua pertanto l'importanza di predisporre misure in grado di presidiare efficacemente sia la fase progettuale dell'utilizzo dei dati in base ai principi del GDPR sia quella inerente alla verifica di un trasferimento ed uso improprio di dati.

Il trasferimento transfrontaliero dei dati è fondamentale per il commercio internazionale, per la gestione dei clienti e la coordinazione integrata dei processi di fornitura[8], quali la prestazione di servizi[9]; tuttavia la sua pervasiva dimensione sfida quotidianamente i diritti alla privacy e alla sicurezza dei dati e stride spesso con le necessità di conformità con il GDPR.

Deve ricordarsi che non solo la protezione dei dati[10] ma anche la loro libera circolazione, purché contenuta entro i limiti del pregiudizio dei diritti della persona, è uno degli oggetti e finalità del Regolamento, nella misura in cui si riferisce ad un mercato unico digitale europeo

Grunes, *Big data and Competition Policy*, OUP, 2016; M.E. Stucke - Azrachi, *When Competitopn Fails to Optimise Quality: A Look at Search Engines*, in *Yale Journal of Law and Technology*, 2016, p. 70; F. Pasquale, *Privacy, Antitrust and Power,* in *20 Geo Mason L. Rev.*, 2013, p. 1009.

[7] Possono essere agenti, partner o responsabili esterni del trattamento.

[8] Si pensi, a titolo esemplificativo, anche al servizio Last - Mile, ossia all'ultima fase del processo di consegna, la parte che consente il raggiungimento del prodotto al consumatore finale, che prevede l'analisi delle opinioni dei consumatori che ha portato alla installazione di sistemi strategici, definiti di pseudo-etichettatura ad alta confidenza che assegnano automaticamente etichette artificiali (pseudo-etichette) ai dati non annotati quando si rileva un livello di confidenza molto elevato nella predizione. Tuttavia, queste strategie indeboliscono le garanzie di sicurezza delle informazioni. Si v. K. Sangbaek - L. Hongchul - K. Jiho, *Efficient opinion mining for imbalanced customer reviews in last-mile services*, in *Data Knowl. Eng.*, 160, 102466, in *https://doi.org/10.1016/j.datak.2025.102466.*

[9] Cfr. A. Addante, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Gius. civ.*, 2020, n. 4, p. 889.

[10] D'altronde, gli stessi addetti ai lavori al Regolamento hanno chiarito la circostanza che il diritto della protezione non rappresenta una prerogativa assoluta, ma deve essere visto alla luce della funzione sociale.

e non globale, dimensione invece attuale dell'economia digitale[11]. La necessità, pertanto, di estendere questa tutela anche fuori dal territorio europeo fa sì che trasferimenti e duplicazioni debbano convivere con il divieto di un predefinito trasferimento di dati. Occorre, pertanto, che siano adottate specifiche precauzioni "su misura", variabili a seconda del flusso di dati coinvolto, con l'obiettivo di garantire che il paese non europeo destinatario dei dati offra garanzie analoghe a quelle del GDPR. Ne consegue che gli Stati sono tenuti ad implementare un'adeguata governance che rispetti i principi della limitazione delle finalità e della minimizzazione dei dati[12], per cui le finalità dell'utilizzo devono essere determinate, esplicite e legittime, rigorosamente nella misura in cui siano limitate a quanto strettamente necessario. Gli strumenti e le pratiche digitali, quali commercio elettronico, cloud computing, social network[13] e blockchain[14] sono solo alcune modalità operative quotidiane che implicitamente richiedono un trasferimento dati fluido.

Il modello cloud computing[15] offre possibilità di condivisione, ar-

[11] L'articolo 1 del GDPR rappresenta l'esatto bilanciamento tra protezione dei dati e mercato unico europeo, per cui deve essere garantita la libera circolazione dei dati e ovviata una frammentazione del mercato interno, senza che la protezione dei dati possa essere in alcun modo causa limitante.

[12] Si v. W. Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, in *Geweblincher Rechtsschutz und Urheberrecht, Internationaker Teil*, 2026, vol.65, n.11, p. 989.

[13] Sul tema della responsabilità dei social network, in particolare, si v. S. Sica, G. Giannone Codiglione, *I social network sites e il labirinto delle responsabilità*, in *Giur. mer.*, 12, 2012, pp. 2714- 2733. è d'uopo pertanto riferire che proprio il caso del social network Facebook ha dato il via all'inchiesta e ai processi, noti come Scherm I e Scherm II, che hanno portato all'attuale decisione di adeguatezza della Commissione europea, che indica minutamente i principi applicativi e le garanzie giudiziarie e stragiudiziali che devono essere offerti in occasione di un trasferimento verso gli Stati Uniti. Si v. V. D'Antonio, *Il trasferimento dei dati all'estero, sub artt. 42-45*, in S. Sica - P. Stanzione (diretto da), *La nuova disciplina della privacy*, Zanichelli, 2005, pp. 155-197.

[14] Cfr. E. Battelli, *Le nuove frontiere della automatizzazione contrattuale tra codici algoritmici e big data: gli smart contracts in ambito assicurativo, bancario e finanziario*, in *Gius. civ.*, 2020, n. 4, p. 681 e ss.

[15] La classificazione dei tipi di storage può essere diversamente compiuta, che comprende: cloud storage privato o personale, se accessibile solo da una organizzazione specifica o da una persona fisica individuata; cloud storage pubblico, ovvero cloud community per

chiviazione e calcolo di dati su richiesta, offrendo tra l'altro benefici finanziari e, in modo conclamato, modalità di ridurre i costi operativi. Rappresenta pertanto un viatico molto rapido per la trasmissione di dati, nonché canale a rischio per la sicurezza informatica[16]. Social network, come piattaforme Meta, TikTok, X, processano costantemente grandi dataset per analizzare i profili e figurare una segmentazione degli utenti, generando rischi di trasferimenti di dati non tracciati e violazioni dei principi di minimizzazione e circoscrizione delle finalità.

La crescente dipendenza dall'intelligenza artificiale[17], dai sistemi di cloud computing e dalla tecnologia della blockchain[18] rende poi ancora più complesso garantire un rispetto della normativa dettata a tutela dei dati, senza considerare che ogni trasferimento dati deve misurarsi con le politiche commerciali e locali, nonché con le possibili intrusioni legittimate da interessi di sicurezza nazionale. Il tema della sicurezza nazionale è spesso il punto nevralgico della regolamentazione del trasferimento dati, soprattutto quando sono coinvolti gli Stati Uniti, su cui intende

la comunità ed infine ibrido cloud computing. T. Alam, *Cloud computing and its role in the information technology*, in *IAIC Transactions on Sustainable Digital Innovation* (ITSDI), 2020, vol. 1, n. 2, pp. 108-115,

[16] A. A. Khan - A. A. Laghari - S. Awan - A. K. Jumani, *Fourth industrial revolution application: network forensics cloud security issues*, in *Security Issues and Privacy Concerns in Industry 4.0 Applications*, 2021, p. 15. B. Wang - B. Li - H. Li, *Knox: privacy-preserving auditing for shared data with large groups in the cloud*, in *Proceedings of the International conference on applied cryptography and network security*, Springer-Verlag, June 2012, pp. 507–525. Cfr. J. Hassan - D. Shehzad - U. Habib - M.U. Aftab - M. Ahmad - R. Kuleev - M. Mazzara *The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges. A Systematic Literature Review (SLR)*, in *Computational Intelligence and Neuroscience*, 2022, Article ID 8303504.

[17] Tuttavia, l'intelligenza artificiale solleva diverse questioni giuridiche, molto legate al tema della responsabilità e al problema della proprietà intellettuale delle informazioni che vengono deliberatamente utilizzate dalla "macchina" una volta inserite. Cfr. G. Pignataro, *La produzione intellettuale dell'IA generativa tra etica e diritto*, in *Dir. pubbl. eur. Rassegna online*, 2024, n. 2, p. 138 e ss.

[18] Un'analisi su alcuni aspetti tecnici quali i "gemelli digitali personalizzati" che consentono di realizzare un'assistenza sanitaria personalizzata attraverso meccanismi avanzati di privacy e sicurezza, si v. A. Shankhdhar - H. Garg, *Blockchain enabled secure data transmission for personalized e-healthcare and digital twin well-being,* in Aa.Vv., *Cluster computing*, 2025, vol. 28 (15), p. 926.

soffermarsi questa analisi, giacché la politica federale statunitense è in modo dominante sbilanciata a favore di invasivi controlli sui dati ed utilizzo degli stessi (all'insaputa degli interessati), a discapito di un utilizzo conforme alle prerogative e garanzie disposte dal Regolamento della privacy[19]. Spesso non è chiaro dove i dati siano fisicamente conservati e trattati, inoltre, i fornitori dei servizi cloud hanno infrastrutture distribuite globalmente, così che i flussi di dati possono trovarsi ad attraversare automaticamente paesi privi di una decisione di adeguatezza della Commissione europea. o comunque ove tale decisione presenta criticità attuative.

Le difficoltà a realizzare una regolamentazione controllata dell'utilizzo dei dati sono emblematicamente rappresentate negli Stati Uniti, con le inevitabili ripercussioni oltreoceano, dal *Clarifying Lawful Overseas Use of Data Act*, noto come *Cloud Act*, legge federale approvata il 23 marzo 2018[20]. Si tratta di una legge dedicata a misurare l'obbligo delle aziende tecnologiche statunitensi di fornire alle autorità l'accesso ai dati, qualunque sia la sede fisica in cui siano archiviati i dati. Questa legge espressamente stabilisce la possibilità per le agenzie governative di poter chiedere, alle telecomunicazioni statunitensi, comunicazioni, dati sul traffico e informazioni sugli abbonati di servizi forniti[21] sollevando un conflitto con il principio di sovranità territoriale e interferendo con gli ordinamenti giuridici extra US, *in primis* quelli europei: uno stru-

[19] Il caso Snowden è emblematico della rilevata incompatibilità tra i programmi di sorveglianza USA e il livello di protezione richiesto dal diritto dell'UE ed è ciò che ha influenzato maggiormente le sentenze Scherms I (C-362-14, 2015) e Scherms II (C-311-18- 2020). Tuttavia, anche il caso Google Spain C- 131/12 2014, che ha portato al riconoscimento del diritto all'oblio, in pratica al diritto di chiedere la deindicizzazione di informazioni personali, rileva i diversi indirizzi politici e giuridici con cui vengono trattati questi interessi spesso contrapposti. Si veda, e*x pluribus*, G. Sartor - M. Viola De Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU*, in *Diritto inf.*, 2014, n. 4 e 5, p. 657.

[20] Cfr. H. Hailu Abraha, *How compatible is the US "Cloud Act" with cloud computing? A brief analysis*, in *International data privacy law*, vol. 9, p. 207; R. Bismuth, *Le Cloud Act face au projet européen e-évidence: confrontation ou coopération?*, in *Revue critique de droit international privé*, 2019, vol. 3, p. 681.

[21] Invero, questa legge aggira anche i tradizionali trattati di assistenza giudiziaria (MLAT). Gli ordini hanno obbligo di segreto, e pertanto comportano il divieto di informare l'utente.

mento che in modo esponenziale accresce il potere dell'intelligence e depaupera i diritti degli individui.

2. La Direttiva 95/46/EC sulla protezione dei dati personali conteneva già in nuce il principio che è alla base del trasferimento dei dati, principio poi sviluppato ed ampliato nella sua portata dal Regolamento GDPR[22].

Il fondamento giuridico di consentire un trasferimento dati solo ove il paese destinatario offra tutela adeguata si rinveniva pertanto già nell'art. 25 della Direttiva 95/46/CE per cui gli Stati membri potevano trasferire verso un paese terzo dati personali, oggetto del trattamento o destinati ad essere trattati successivamente, solo se il paese terzo in questione garantisse un livello di protezione adeguato e purché fossero rispettate le disposizioni nazionali di recepimento della Direttiva[23].

Il Regolamento GDPR ha ampliato l'ambito territoriale di applicazione anche ai soggetti extra Unione Europea, aspetto centrale di questa analisi, nonché ha esteso la portata di questa legge anche ai titolari e contitolari stabiliti fuori dall'UE che però trattano dati di "interessati"

[22] Si v. V. D'Antonio, *Il trasferimento dei dati all'estero, sub artt. 42-45*, in S. Sica - P. Stanzione (diretto da), *La nuova disciplina della privacy*, cit., pp. 155 - 197.

[23] Così art. 25 Direttiva 95/46/CE. Si ponga mente che le cornici in cui si inserisce questa norma ossia, l'art- 16, paragrafo 1 del Trattato sul funzionamento europeo per cui «tutti hanno diritto alla protezione dei dati personali che li riguardano» e l'art. 8 della Carta dei diritti fondamentali dell'Unione Europea per cui, alla luce del primo comma, «tutti hanno diritto di protezione dei dati personali che li riguardano». Dal secondo comma, si evince che «tali dati devono essere trattati in modo corretto per finalità determinate e sulla base del consenso dell'interessato o di un'altra base legittima fissata dalla legge». Ogni persona ha il diritto di accedere ai dati che la riguardano e di farli rettificare. Ai sensi del terzo comma, invece, è opportuno che il rispetto delle regole (stabilite dai precedenti commi) sia soggetto al controllo da parte dell'autorità indipendente. E ad ogni modo, occorre un'interpretazione combinata con l'art. 4 della medesima Direttiva che determina quale legge nazionale di protezione dati si applica ad un determinato trattamento. Sostanzialmente l'art. 4 stabiliva quale Stato membro fosse competente ad applicare la propria legge nazionale sulla protezione dei dati quando il trattamento presenta profili di internazionalità. Per un'analisi dell'interazioni di queste due norme della Direttiva, soprattutto alla luce delle pronunce della Corte di Giustizia Europee, ante operatività GDPR, si v. M. Gömann, *The new territorial scope of EU Data Protection LAw: Decostructing a Revolutionary Achievement*, in *Common Market Law Review*, 54:567-590, 2017.

che si trovano nell'UE (ai sensi dell'art. 3 GDPR). Questo rappresenta un punto di partenza estremamente importante, chiarito il quale è possibile investigare sulle garanzie richieste dall'Unione Europea perché sia possibile un trasferimento dati senza ledere i diritti degli interessati, i cui dati sono oggetto di trattamento.

Sin da subito occorre dire che, se le regole di decisioni di adeguatezza della Commissione Europea, disposte dall'art. 45, hanno ripreso integralmente l'art. 25 della Direttiva, non altrettanto si può dire delle altre eccezioni o garanzie per i trasferimenti, disposti dagli artt. 46-49 del GDPR, quali, a titolo esemplificato, le clausole contrattuali tipo o le norme vincolanti d'impresa.

Ma prima ancora di una possibile disamina di decisioni di adeguatezza, occorre porre mente al criterio territoriale con cui esse devono convivere, criterio disciplinato dall'art. 3 del GDPR. In questi termini, essa appare come una dichiarazione di principio.

L'obiettivo è di offrire una garanzia effettiva, pertanto, nessuna valenza concreta viene attribuita alla sede legale dell'organizzazione, rilevando il luogo dello stabilimento o il concreto impatto sui cittadini europei di tale uso dei dati. I dati personali devono essere trattati nell'ambito delle attività di uno stabilimento o di un titolare situato nell'Unione e indipendentemente dal luogo in cui avviene il trattamento o dal se l'interessato si trovi o meno nell'UE[24]. Quindi, qualora lo stabilimento si trovi nell'Unione Europea, il trattamento dei dati deve essere conforme al GDPR anche se il trattamento avvenga fuori dalla Unione Europea. È necessario che vengano però soddisfatte precise condizioni; pertanto, la semplice accessibilità di un sito web nell'Unione non è di per sé idonea a far scattare queste condizioni. Il trattamento

[24] Ad esempio, nella sentenza *Google Spain*, la Corte di giustizia ha applicato al motore di ricerca di Google l'articolo 4(1)(a) della DPD (equivalente all'art. 3(1) del GDPR), che riguardava il trattamento dei dati effettuato «nell'ambito delle attività di uno stabilimento» di un titolare situato in uno Stato membro, nonostante l'operatore effettivo del motore di ricerca e il titolare del trattamento si trovassero in un paese terzo. La Corte ha quindi stabilito in quell'occasione che il trattamento di dati personali da parte di un motore di ricerca gestito da un'impresa con sede fuori dall'UE, ma dotata di uno stabilimento in uno Stato membro, era effettuato «nell'ambito delle attività» di tale stabilimento e rientrava pertanto nell'ambito di applicazione del diritto dell'UE in materia di protezione dei dati.

deve essere connesso all'offerta di beni o servizi ad interessati che si trovano nell'Unione o deve essere applicato ai titolari e responsabili del trattamento senza uno stabilimento nell'UE quando le attività svolte sono collegate al monitoraggio del comportamento degli interessati nell'UE e nella misura in cui tale comportamento abbia luogo all'interno dell'Unione[25].

Ne consegue che un'azienda francese che abbia un server negli Stati Uniti deve agire in conformità del GDPR anche qualora i dati si riferiscano a persone che si trovano stabilmente nel territorio statunitense. Una società statunitense che vende prodotti a clienti residenti nell'UE deve raccogliere i dati personali dei consumatori nel rispetto del GDPR. Se poi i dati vengono successivamente trasferiti ad un server dell'azienda o ad un fornitore di servizi che si trova in un altro paese terzo, subentra l'operatività di quanto disposto dal Capo V del GDPR, ossia in merito al «trasferimento internazionale verso paesi terzi o organizzazioni internazionali»[26]. In questo caso, occorre una decisione di adeguatezza adottata dalla Commissione europea, o in alternativa, devono essere usate clausole contrattuali standard (SCC) o regole vincolanti d'impresa (*Binding Corporate Rules*, BCR) o altra forma di garanzia adeguata ai sensi degli artt. 46-49. Le misure alternative alle decisioni di adeguatezza richiedono, però, il *Data Transfer Impact Assesment*, ossia una valutazione dei rischi più approfondita.

[25] Il Regolamento però si applica anche quando il trattamento dei dati è effettuato da un titolare o responsabile non stabilito nell'Unione europea se però si applica il diritto di uno Stato membro in virtù del diritto internazionale europeo. Esempi tipici sono ambasciate, consolati di Stati membri, navi che battono bandiera di uno stato membro, aeromobili immatricolati in uno stato. Ne consegue che tutti i trattamenti posti in essere nell'esercizio di funzioni ufficiali di uno Stato membro sono giuridicamente riconducibili a quello Stato.

[26] L'introduzione di queste disposizioni, in occasione del GDPR, è nata proprio dal timore, che era presente con la Direttiva della protezione dei dati, di una insufficiente protezione dei dati personali trattati o trasferiti al di fuori dell'UE. Nasce proprio la necessità di considerare anche le circostanze in cui i titolari e i responsabili del trattamento non sono stabiliti nell'UE ma il trattamento è connesso all'offerta di beni e servizi a "interessati" che si trovano nell'Unione

Ad ogni modo, le interpretazioni della Corte di giustizia dell'Unione europea[27] sono state molto importanti, disponendo l'applicazione del GDPR a situazioni transfrontaliere che, a prima vista, potevano sembrare escluse dal perimetro applicativo. Il caso eclatante, e molto rappresentativo della criticità del tema, è il trattamento dei dati da parte dei servizi di intelligence degli Stati membri che esulano dagli scopi del diritto dell'Unione; questo può presentare delle forti criticità poiché le attività dei servizi possono esplicarsi nel tentativo di accedere a dati raccolti da operatori privati per finalità commerciali. La Corte ha stabilito che tale accesso rientra nel diritto dell'UE e ha anche specificato che il fatto che i dati possano essere trattati dalle autorità di un paese terzo per ragioni di sicurezza pubblica, sia essa difesa o sicurezza dello Stato, non consente di eludere l'applicazione del GDPR. In questi termini, essa appare però come una dichiarazione di principio. Il binomio sicurezza-tutela dati presenta evidenti fragilità in un'analisi di trasferimento dati Europa- Stati Uniti.

Ed è tal riguardo che è di particolare interesse vedere l'interazione tra quanto disposto dalle norme in ambito territoriale e quanto disposto da quelle sul trasferimento transfrontaliero dei dati (Capo V, GDPR), giacché mentre l'art. 3 si applica indipendentemente dal livello di protezione presente nello stato terzo, le norme del Capo V sono proattive e richiedono pertanto a terzi l'adozione di determinate misure e garanzie prima che sia compiuto il trasferimento. È bene porre in mente che nei due noti giudizi Schrems[28] della Corte di giustizia, sebbene riguardino le pratiche di trasferimento dati verso paesi terzi di Facebook, sia stato anche rilevato che Facebook avesse utilizzato plug-in e cookies per tracciare e identificare gli utenti, e che pertanto tale trattamento rientrasse anche nell'ambito territoriale della normativa UE sulla protezione dei dati (indipendentemente da un comportamento proattivo del paese terzo).

Anche in ragione di queste sovrapposizioni, il Comitato Europeo dei Dati personali (EDPB) nel novembre 2021 ha adottato linee guida

[27] Cfr. TEU, art. 4 (2).

[28] Si veda sentenza della Corte di giustizia europea del 6 ottobre 2015, C-362/14 (Sherms I) e la sentenza del 16 luglio 2020, C-311/18 (Scherms II).

proprio in merito alla interazione tra «l'ambito territoriale» e le «norme sui trasferimenti dati» definendo i requisisti di un trasferimento internazionale di dati. Ha enucleato la necessità che l'importatore dei dati sia situato in un paese terzo, salvo che si tratti un'organizzazione internazionale, Ha inoltre chiarito la necessità che la comunicazione dei dati e la loro messa a disposizione siano compiute da un titolare o responsabile del trattamento soggetto al GDPR. Il Comitato ha inoltre precisato che la trasmissione dei dati deve essere rivolta ad altro titolare o responsabile del trattamento, non riscontrandosi pertanto alcun trasferimento degli stessi «quando i dati sono comunicati direttamente e su iniziativa propria dall'interessato». Ad ogni modo, agli interessati che hanno assunto personalmente l'iniziativa è concesso il diritto di presentare un reclamo a un'autorità di protezione dei dati (DPA), ai sensi dell'art. 77, o a un tribunale (art. 79) nello Stato membro ove il titolare o il responsabile abbia lo stabilimento, ovvero l'interessato risiede. Tuttavia, il rimedio di ricorrere all'autorità di controllo non si rileva particolarmente efficace soprattutto quando la parte coinvolta non abbia anche una sede in Europea, visto che l'ambito operativo di un'autorità garante ha il limite del territorio nazionale. Per di più, la nomina di un rappresentante da parte di soggetti non europei non aiuta ad irrobustire la valenza operativa dell'art. 3, posto che la responsabilità del rappresentante è sempre limitata agli obblighi diretti previsti dagli artt. 30 e 58, comma uno, lettera a) del GDPR e non sostituisce quella del titolare o del responsabile del trattamento che rappresenta.

Ed è per questo che in presenza delle condizioni, che consentono di applicare gli artt. 45 e ss. del GDPR, questi ultimi si rivelano più convenienti, soprattutto in termini rimediali, quando appunto si verifica la non conformità alla decisione di adeguatezza e alle garanzie riconosciute.

3. L'analisi delle condizioni perché possano essere legittimamente trasferiti i dati nei paesi extra Unione Europea nel rispetto delle garanzie del GDPR ed in particolare, il rapporto EU- USA, è un tema in continua evoluzione dal punto di vista dell'enforcement, ossia della idoneità delle regole ad essere ben rispettate. Come si è anticipato, le

modalità per un trasferimento dati, rispettose dei principi del GDPR, sono numerose e le circostanze, sebbene talvolta sovrapponibili alle circostanze indicate dall'art. 3, inducono a preferire l'applicazione del Capo V.

Senz'altro le decisioni di adeguatezza disposte dalla Commissione Europea ai sensi dell'art. 45 del GDPR rappresentano i requisiti e i parametri determinanti in un'analisi di trasferimento dati verso Stati Uniti.

Queste "decisioni" sono racchiuse in un provvedimento con cui la Commissione stabilisce che un Paese terzo, un particolare territorio o settore specifico, assicura un livello di protezione dei dati equivalente a quello previsto dal GDPR. La presenza di tali decisioni di adeguatezza è formalmente sufficiente per legittimare il trasferimento dati e non necessita di ulteriori garanzie aggiuntive. Tuttavia, talune criticità dei profili attuativi di una decisione di adeguatezza possono indurre talvolta a preferire la strada di utilizzare strumenti alternativi, come accade negli Stati Uniti, posto che la volontà di avvalersene richiede alle imprese numerosi adempimenti. Difatti, sebbene la Commissione abbia adottato una decisione di adeguatezza e ci siano stati diversi interventi correttivi ed integrativi, proprio al fine di garantire la concretezza di tali finalità di garanzia, alcune aziende preferiscono optare per le "clausole contrattuali tipo", anche perché la decisione di adeguatezza richiede un'adesione da parte delle imprese, adesione approvata solo dopo che sia stata data prova di numerosi adempimenti[29] che si rilevano molto restrittivi, esclusivi di numerosissime attività, senza considerare che la concessione è subordinata al previo pagamento di una elevata *fee*. I requisiti di eleggibilità comprendono la necessità di essere un'entità sotto il controllo della *Federal Trade Commission* o sotto il controllo del Dipartimento dei Trasporti statunitense, il che di fatto comporta la non eleggibilità di molte entità che svolgono attività economiche, seppur non strettamente commerciali, come, a titolo esemplificativo, le istituzioni bancarie o

[29] Le attività di compliance posso avere diverse forme: la compliance formale richiede un autocertificazione annuale, la dichiarazione di adesione ai principi ai DPF *Principles* e l'inserimento nella DPF List ufficiale; la compliance sostanziale richiede l'adozione di policy interne conformi ai DPF Principles, l'adeguamento alle procedure di trattamento, e l'adozione di meccanismi di *data minimization*, *purpose limitation* e *security*; e infine, la compliance di controllo che include anche i meccanismi di reclamo e di ricorso per gli interessati.

le organizzazioni non profit. In aggiunta, il "certificato di adesione", *Data Controller Certification*, rilasciato dal Dipartimento di commercio statunitense (DoC) ha una valenza annuale, il che determina l'obbligo di nuove valutazioni cadenzate annualmente. Gli strumenti giuridicamente vincolanti e alternativi alla decisione di adeguatezza sono differenti a seconda delle circostanze e i più ricorrenti sono le clausole contrattuali tipo e quelle vincolanti di impresa, proprio perché talvolta in grado di assicurare misure di sicurezza più adeguate alla conformità alle prescrizioni dell'Unione Europea. Sono clausole che impongono obblighi contrattuali sia agli esportatori che agli importatori di dati e devono essere approvate dall'Autorità europea dei dati.

L'attenzione rivolta negli ultimi venti anni alla gestione statunitense dei dati europei è stata ripetuta e progressiva. D'altronde, come è noto, le prime negoziazioni tra l'Unione Europea e gli Stati Uniti d'America hanno origine nelle note vicende giudiziarie che hanno dato vita al "Safe Harbor principle", ossia alla redazione di un accordo tra la Commissione Europea e gli Stati Uniti volto a garantire un livello adeguato di protezione dei dati nella fase di archiviazione, analisi e utilizzazione da parte dei servizi emergenti della società dell'informazione, come i servizi di fornitura di contenuto digitale ed i social network. Questo accordo è stato annullato dalla nota sentenza della Corte di Giustizia Europea (Causa C-362/14), conosciuta come Scherms I[30], perché ritenuto inadeguato a garantire una protezione contro la sorveglianza governativa USA e non in grado di offrire ai cittadini europei strumenti efficaci per far valere i propri diritti[31]. La questione, in particolare, era

[30] Case C-362/14, Scherms v. Data Prot. Commissioner, 6 Ottobre 2015. Questa pronuncia ha esaminato se la decisione della Commissione 2000/520/CE (con la quale fu dichiarata l'adeguatezza degli US per i trasferimenti dati) fosse valida alla luce della Direttiva 95/46/CE e degli articoli 7 e 8 della Carta dei Diritti Fondamentali. Si v., *ex pluribus*, F. Rossi Dal Pozzo, *La tutela dei diritti personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbour al Privacy Schield)*, in *Riv. dir. int.*, 2016, n. 3, p. 690.

[31] In particolare, al punto 141 dell'opinione dell'avvocato generale nella causa Scherms (C-362/14) della Corte di Giustizia dell'Unione Europea è stata evidenziata la necessità di offrire condizioni concrete per assicurare un adeguato livello di protezione che deve quindi essere sostanzialmente equivalente.

stata sollevata da Maximilliam Scherms, un attivista austriaco, utente di Facebook Irlanda, che aveva contestato l'inadeguatezza del trasferimento dei dati degli utenti europei a Facebook America. La Corte ha riscontrato che il trasferimento compiuto verso la americana Facebook Inc era stato compiuto senza che ci fosse stato un previo accertamento delle adeguate garanzie e senza che fossero raggiunti gli standard richiesti dall' UE. La criticità era stata poi acuita dal trasferimento di questi dati alla Agenzia della Sicurezza Nazionale, sulla base del programma PRISM, che consentiva il diritto illimitato di intercettazioni e ricerca dati sotto lo scudo della sicurezza nazionale.

Base del giudizio promosso da Scherms è la violazione degli artt. 7 e 8 della Carta fondamentale dei diritti dell'uomo[32] da parte di *Facebook Ireland* nel trattamento dei dati personali dei propri utenti.

Questa invalidazione ha comportato l'obbligo delle aziende, che intendevano processare dati, di ottenere una autorizzazione speciale europea che consentisse loro l'utilizzo dei dati. Questo iter era stato molto dispendioso perché comportava tempi lunghi, legati anche alla necessità di duplicare server[33]. Di qui la necessità di avviare un nuovo processo negoziale per trovare una definizione d'intesa negoziale conforme ai requisiti di legittimità ex GDPR che ha visto la luce nel luglio 2016 con il *Privacy Shield Agreement*, conosciuto come *Privacy Shield 1.0* con il quale furono ulteriormente specificati i requisiti e i nuovi standards per assicurare un flusso di dati sicuro verso gli Stati Uniti e, in particolare, fu istituita la *Privacy Schield Ombudsman*.

Questa figura, nominata dal potere esecutivo e deputata a dirimere i reclami relativi al trattamento improprio dei dati personali da parte

[32] Come è noto mentre l'art, 7 sancisce il rispetto alla vita, alla famiglia e alle comunicazioni personali, l'art. 8 garantisce il diritto alla protezione dei dati personali e garantisce come questi debbano essere trattati e controllati, ossia secondo il principio di lealtà, in base al consenso della persona interessata o in ragione di altro fondamento legittimo previsto dalla legge, il tutto con la necessità che tali regole siano soggette al controllo di un'autorità indipendente , fatto sempre salvo il diritto dell'interessato di accedere ai dati raccolti che lo riguardano e di ottenere la rettifica.

[33] T. Katulic - G. Vojkovic, *From safe harbour to European data protection reform*, in *39th International Convention on Information and Communication Technology Electronics and Microelectronics* (MIPRO) 2016, IEEE, p. 1147.

di società statunitense, fu subito molto criticata per non incarnare i caratteri propri dell'imparzialità e dell'indipendenza, necessari per una valutazione corretta dei reclami relativi al trattamento improprio dei dati personali da parte di società statunitensi.

Ad ogni modo, sia il *Privacy Schield 1* che l'*Ombunsman* hanno avuto vita breve. L'accordo (*Privacy Shield 1.0*) è stato difatti invalidato dalla Corte di giustizia dell'Unione europea nel noto caso "Scherms 2", causa C-311/18. L'operatività del *Ombudsman* è stata invece sostituita dalla *Data Protection Review Court*, istituita con ordine esecutivo sotto la Presidenza Biden nel 2022, che ha avuto un impatto significativo sul trasferimento transatlantico di dati. Nel decidere la causa C-311/18, invero, con sentenza del 16 luglio 2020, la Corte è andata al di là della verifica in US dell'inadeguatezza del livello di protezione "sostanzialmente equivalente" a quello richiesto dal diritto dell'Unione europea, e ha evidenziato il punto nevralgico degli Stati Uniti, nascosto sotto lo scudo della sicurezza. La Corte ha rilevato come il quadro normativo statunitense consenta pratiche di sorveglianza generalizzata incompatibili con i principi di necessità e proporzionalità, sanciti dagli artt. 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione Europea. In particolare, vengono posti in rilievo l'Ordine Esecutivo n. 12333 del 1981 firmato dall'allora presidente Ronald Regan[34], la Sezione 702 del *Foreign Intelligence Surveillance Act* (FISA) del 2008 e la Direttiva presidenziale n. 28 del 2014, tutti strumenti che abilitano e legittimano le agenzie di intelligence statunitensi ad anteporre il diritto alla sicurezza a qualunque diritto della persona, contenuto ed espresso nella tutela dei dati, con un disallineamento evidente con la normativa europea.

Nella stessa decisione è stata anche sottolineata invece l'idoneità delle clausole contrattuali tipo che possono prevedere garanzie aggiuntive qualora si verifichi che le stesse da sole non siano sufficienti per garantire un'adeguata protezione ai sensi del diritto dell'UE.

Questa seconda invalidazione ha portato ancora una volta a nuovi negoziati conclusisi con la dichiarazione di adeguatezza nota come

[34] Si tratta di uno dei documenti centrali della regolamentazione della attività dell'intelligence statunitense, attraverso le definizioni e responsabilità delle diverse agenzie (CIA, NSA, FBI, e via enumerando).

Data Privacy Framework, nuovo accordo adottato il 10 luglio 2023, conosciuto anche come "Privacy Schield 2.0" sul quale si intende compiere alcune riflessioni.

4. Nel periodo di vacanza di una "decisione di adeguatezza" l'Europa, attraverso il Comitato Europeo per la protezione dei dati (EDPB), ha elaborato un corpus di raccomandazioni sui meccanismi di trasferimento aggiuntivi per garantire che questi flussi transatlantici fossero in grado di offrire un'adeguata protezione. Inoltre, il Garante europeo per la protezione dei dati[35](GEPD), noto come *l'European Data Protection Supervisor*, ha fornito ulteriori indicazioni sul trasferimento dei dati aggiornando anche le "clausole contrattuali tipo" per il trasferimento di dati, chiarendo i principi su cui esse debbono fondarsi, con indicazione della necessità di munirsi di misure supplementari, quali la crittografia, la pseudonimizzazione, la valutazione del rischio per garantire una conformità continua. Il che ha comportato per le multinazionali l'obbligo di munirsi di una governance interna, adottando procedure di due diligence rafforzate e incorporate in garanzie contrattuali conformi al GDPR.

Il *Data Privacy Framework* ha anche beneficiato dell'ordine esecutivo n. 14986 del 7 ottobre 2022 intitolato *Enhancing Safeguards for United States Signals Intelligence Activities*, adottato (durante la Presidenza Biden) principalmente in risposta alle critiche della Corte di Giustizia dell'UE nella sentenza Scherms II con le quali erano stata rafforzata la tutela per le attività di raccolta di intelligence sui segnali elettromagnetici, stabilendo che le attività di intelligence devono essere necessarie, proporzionate, in particolar modo quando sono coinvolti dati personali di cittadini non statunitensi, e strettamente finalizzate esclusivamente ad obiettivi di sicurezza nazionale chiaramente definiti conformemente a quanto disposto dalla legge relativa alla vigilanza sull'intelligenza

[35] Tra le sue funzioni vi è il compito di controllare che le istituzioni europee rispettino il diritto alla protezione dei dati; inoltre, collabora con le autorità nazionali per garantire coerenza nell'applicazione delle norme sui dati personali nell'UE e gestisce reclami degli interessati nei confronti del trattamento dei loro dati da parte degli organismi dell'UE.

esterna (FISA) o dalla disposizioni di legge che autorizzano l'accesso attraverso cosiddette *National Security Letter* (NSL)[36].

L'ordine esecutivo n. 14086 enuclea l'importanza della "raccolta mirata", quale uno dei principi centrati del GDPR, espressi dal binomio finalità-minimizzazione, per cui il trattamento del dato deve essere consentito per una specifica finalità e deve essere minimizzato (a livello tempistico e non solo) per il raggiungimento di quella determinata finalità[37]. A tal fine l'*Executive Order* incide sulla *Presidential Policy Directive 28*, non escludendo, tuttavia, la sorveglianza di massa. La sez. 702 *Foreign Intelligence Surveillance Act* (FISA) 50 U.S.C. e *l'Executive Order* n.12333 rimangono invariati malgrado la Corte di Giustizia (nella decisione Schrems II) avesse espressamente sancito che la sorveglianza di massa non rispetta il principio di proporzionalità e avesse mostrato diffidenza nei confronti di queste disposizioni proprio perché troppo generiche e non delimitate come richiesto dagli artt. 7 e 8 della Carta dei diritti fondamentali. Ne consegue che non sorprende come possano palesarsi elevati rischi di svuotare di legittimità il trattamento dei dati personali laddove sia offerta ampia discrezionalità alle ingerenze nell'utilizzo di dati. Non può negarsi che tale ordine abbia potuto creare le basi per un quadro di riferimento, oltre che dichiaratorio di principi, anche garante di una tutela effettiva con l'intento di offrire un sistema di controllo preventivo e successivo, attraverso rimedi giudiziari e stragiudiziali, volti a consolidare effettivamente gli impegni assunti nei confronti dell'UE. Tuttavia, sempre in atto è la sfida in merito all'attuazione di un bilanciamento tra sicurezza e tutela dei diritti fondamentali, tra privacy, sicurezza e sovranità digitale. L'UE è un sistema fondato sui diritti fondamentali, riconosciuti e tutelati sia a livello primario che secondario, ed oggi costruito anche sulla tutela dei dati, quale diritto distinto con una propria identità, che può

[36] Cfr. Considerando n. 121 del DPF e Codice degli Stati Uniti, articolo 3414, titolo 15, articoli 1681u- 1681v e titolo 18, art. 2709.

[37] Inoltre, bisogna anche considerare le tecnologie progettate per ridurre al minimo la raccolta dei dati personali, le cc.dd. *Privacy Enhancing Technologies* (PETs) adottate in conformità del principio privacy by design, previsto dall'art. 25 GDPR, con l'obiettivo di tutelare il dato per tutto il suo ciclo di vita fin dalla progettazione per cui la tutela della privacy e la tutela dei dati devono essere nel progetto di un sistema.

estrinsecarsi nel diritto alla privacy ma non necessariamente. La scelta di dedicare due differenti articoli (artt. 7 e 8) non è casuale ma riflette la volontà di conferire alla protezione dei dati personali e alla tutala del diritto alla privacy un'autonomia concettuale. Negli Stati Uniti invece tutto prende le mosse dal IV emendamento, ossia dalla tutela alla privacy, intrecciata costituzionalmente al diritto federale che legittima intrusioni ed ispezioni che invadono la sfera privata. La tutela dei dati non vive di luce propria, ma quale estensione del diritto alla privacy, e nell'ambito di questa cornice concettuale e costituzionale diversa, e in considerazione anche degli avvenimenti storici, quali quelli terroristici, si comprende come la sicurezza e i controlli di massa siano una questione sempre aperta e molto delicata che costituisce l'anello debole del rapporto di fiducia EU-USA. Inoltre, le leggi federali speciali che da diverse prospettive interferiscono sull'utilizzo dei dati non agevolano la composizione di una regolamentazione uniforme del settore. Si pensi alla *Health Insurance Portability and Accountability Act* (HIPAA) che impone precauzioni specifiche sulla protezione dei dati sanitari dei pazienti o, in materia finanziaria, al *Gramm- Leach -Bliley Act* (GLBA) riservato ai piani di sicurezza informatica e protezione dei dati finanziari, o ancora al *Children's Online Privacy Protection Act* (COPPA) rivolto alla protezione dei dati dei bambini di età inferiore ai tredici anni.

L'*Electronic Communications Privacy Act* (ECPA) del 1986 e il *Stored Communications Act* (SCA) del 2015[38], poi, ancora in vigore, sono particolarmente rilevanti nell'accelerato odierno sistema digitale. Il primo riguarda l'intercettazione delle comunicazioni elettroniche e l'accesso ai dati conservati dai fornitori di comunicazione, il secondo disciplina l'accesso da parte delle autorità statunitensi a contenuti di comunicazioni archiviate e ai metadati. Entrambi teoricamente impongono limiti formali all'accesso delle autorità, subordinandolo a mandati e ordini giudiziari. Limitano le intercettazioni di comunicazioni elettroniche

[38] Lo *Stored Communications Act* è stato comunque modificato nel 2018 dal c.d. *Cloud Act* che prevede l'obbligo delle aziende soggette alla giurisdizione statunitense a consegnare dati richiesti da un'autorità statunitense, anche nel caso in cui tali dati siano conservati fuori dagli Stati Uniti; questa regola comprende qualsiasi modalità: e-mail, messaggistica file cloud o metadati.

con grande impatto sulla sicurezza dei dati in transito o immagazzinati, tuttavia, le soglie di accesso sono molto basse, soprattutto per i cittadini non statunitensi.

Cybersecurity Information Sharing Act (CISA) favorisce la condivisione di informazioni su minacce informatiche tra il settore privato e quello pubblico, con impatti sulla privacy dei dati condivisi, ossia sulla condivisione di dati tra imprese private e governative che devono attuare politiche di cybersecurity.

Particolarmente indicativi delle complessità realizzative di una regolamentazione controllata dell'utilizzo dei dati è poi, come si è anticipato, il *Cloud Act*, legge emanata nel 2018 proprio al fine di fornire chiarezza e certezza legale sull'accesso dei dati elettronici da parte delle autorità, soprattutto quando questi dati sono conservati al di fuori degli US. Questa legge modifica lo *Stored Communications Act* intervenendo proprio sull'aspetto più critico consentendo alle autorità statunitensi la possibilità di richiedere ai provider servizi elettronici e ai cloud la consegna di dati laddove sia stato emesso un mandato valido o altro ordine legale valido, indipendentemente dal luogo fisico in cui i dati sono stati archiviati e quindi anche se archiviati all'estero. Il rischio di un'ingerenza extraterritoriale e di problematiche di *compliance* con le leggi straniere sono evidenti. Questa apparente chiarificazione invero solleva molte perplessità giacché lo stesso testo prevede inoltre la possibilità dei provider di impugnare un ordine di divulgazione qualora rappresenti una violazione delle leggi straniere ed in particolare dei diritti alla privacy di altri paesi. Il *Cloud Act* autorizza però gli US a stipulare accordi bilaterali esecutivi con altri paesi per regolare l'accesso agli atti; e questi accordi di fatto consentono di inviare richieste dirette ai provider senza dover passare per i tradizionali trattati di mutua assistenza legale ossia il MLAT (*Mutual Legal Assistance Treaty*). L'intento è di schivare controversie con leggi straniere sulla protezione dati, giacché il rischio di conflitti è molto elevato e l'impugnazione può essere complessa e lunga, oltre ad accentuare la carenza di trasparenza per i cittadini stranieri.

5. Alla luce di questo inquadramento dei principali interventi che afferiscono alla disciplina dei dati nel diritto statunitense, è possibi-

le soffermarsi sulla struttura dell'ultima dichiarazione di adeguatezza, adottata dalla Commissione europea, ovvero sul *Data Privacy Framework*, datato luglio 2023.

Esso si fonda su un impianto normativo articolato in sette principi fondamentali che rappresentano il *core* e sedici principi addizionali o supplementari che estendono e chiariscono i primi, favorendone l'adattamento ai casi pratici specifici. Se i primi, i principali, riprendono i punti cardine introdotti con il GDPR, i secondi offrono chiarificazioni operative, stabiliscono eccezioni e deroghe, aiutando le imprese a gestire casi difficili o che presentano peculiarità, come il trattamento di dati sensibili, o comunicazioni giornalistiche, responsabilità in contesti contrattuali o investigazioni interne. Sono guide operative, molto importanti soprattutto nella definizione delle eccezioni lecite, e assumono spesso funzioni integrative nei confronti di quelle principali. La trasparenza, ossia l'obbligo di fornire un'adeguata informativa su finalità, categorie di dati e diritti degli interessati può aver bisogno dei principi supplementari per comprendere l'operatività di questo obbligo nei confronti dei dati raccolti offline, o raccolti in contesti giornalistici. La scelta, ossia il consenso, quale secondo principio, deve definire come e quando l'interessato può opporsi o deve dare il consenso, compiendo scelte specifiche, mentre i principi supplementari consentono di chiarire quando serve opt-in, ossia un consenso attivo, oppure è possibile un opt-out, ovvero considerare il consenso dato di default, o ancora occorrono altre forme di consenso, in ragione della specificità dei dati coinvolti. Il terzo principio è quello della responsabilità del trasferimento successivo a terze parti e pertanto della responsabilità del titolare USA che necessita dei principi supplementari che indirizzano verso l'introduzione delle clausole contrattuali, obblighi di minimizzazione o di responsabilità del fornitore. Il quarto principio impone alle imprese di adottare misure di sicurezza, tecniche e organizzative adeguate che devono comunque essere contestualizzate agli scenari e ai settori specifici; l'obiettivo principale è la protezione dalla perdita, distruzione, uso improprio, accesso non autorizzato o alterazione o distruzione del dato. Il quinto principio è spesso definito nella espressione inglese *data integrity § purpose limitation* ed arricchisce quelli precedentemente indicati,

giacché intende render certo che ci sia il rispetto della limitazione delle finalità, della minimizzazione e aggiornamento dei dati. L'accesso deve essere "necessario e proporzionato", principio però, si anticipa, ritenuto vanificato dalla genericità degli obiettivi sottesi ed indicati all'intervento di sicurezza. Vi è poi il principio definito "access principale" che ha l'obiettivo di garantire all'individuo, i cui dati vengono processati, di accedere, correggere e cancellare i propri dati; occorre però porre mente alle eccezioni, contemplate, come per esempio il segreto industriale o la sicurezza nazionale che devono essere misurati e valutati attraverso i principi supplementari. Infine, l'ultimo principio, impone un meccanismo di tutele attraverso l'istituzione di ricorsi, arbitrati, e altri strumenti di tutela ed *enforcement*. Sebbene l'elencazione di questi principi abbia avuto il precipuo scopo di creare un sistema coerente in grado di garantire il requisito europeo di un'equivalenza sostanziale a fronte delle molteplici sollecitazioni della Corte di giustizia europea, la centralità del tema deve essere colta nei rimedi giudiziali e stragiudiziali, offerti parallelamente a adempimenti "amministrativi" articolati su un sistema di autocertificazione. Quest'ultimo è subordinato all'assoggettamento dei poteri di indagine e di esecuzione della Commissione federale per il commercio (FTC) o del Dipartimento dei Trasporti (DOT) degli Stati Uniti. Questa autocertificazione è sottoposta poi ad una verifica in ordine alla veridicità delle informazioni rese, che comunque necessitano di un'ulteriore verifica annuale che deve consentire di confermare l'inserzione dell'organizzazione nella lista di coloro che sono legittimati a beneficiare della decisione di adeguatezza che nasce, si badi bene, anche come strumento di promozione dello sviluppo del commercio internazionale in conformità del codice degli Stati Uniti (titolo 15, art. 1512). La Corte di Giustizia dell'Unione a più riprese ha evidenziato l'importanza che il soggetto interessato possa verificare l'adeguato trattamento dei propri dati qualora ci siano legittimi dubbi sulla violazione dei principi del GDPR ed è in questa prospettiva che è enunciato nel DPF la necessità di un meccanismo di ricorso indipendente, in una forma di doppio grado di giudizio.

Prima ancora che si instauri un "giudizio", la *Federal Trade Commission* deve essere chiamata a compiere un'analisi dei casi che le posso-

no essere sottoposti da un organo di composizione di risoluzione delle controversie o da Stati membri per verificare se il trasferimento dei dati abbia comportato la violazione della sezione 5 del *Federal Trade Commission Act* (15 U.S.C. § 45). Inoltre, la FTC può ottenere un provvedimento amministrativo inibitorio o presentare denuncia presso un giudice distrettuale federale. La eventuale non conformità dell'organizzazione alla decisione dell'ente pubblico o un reiterato comportamento non conforme al DPF UE-USA può comportare la cancellazione dell'organizzazione dall'elenco e soprattutto l'obbligo di restituire e cancellare le informazioni personali ricevute nell'ambito del regime.

Il sistema di autocertificazione, apparentemente semplice, di fatto si rivela non in grado di offrire stabilità nella gestione dei flussi dei dati in ragione del poco agile coordinamento del sistema dei controlli che, oltre ad essere frequenti, sono onerosi sia per le organizzazioni che per gli organi ad essi deputati. La presenza delle condizioni perché ci sia un trasferimento dati sicuro e adeguato alle garanzie offerte dal GDPR è la premessa per ammettere un trasferimento dati verso gli Stati Uniti, che coinvolge le organizzazioni interessate. Ma dalla prospettiva dell'interessato occorre che sia garantito un controllo sul dato per tutto il suo iter di vita e quindi occorre che siano offerti rimedi di controllo, verifica, reclamo qualora ci siano dubbi sull'adeguatezza del trattamento dati. I rimedi non sono propriamente giudiziali, ma meglio definibili quali rimedi stragiudiziali rafforzati perché offerti da un meccanismo non strettamente indipendente ma considerato sufficiente dalla Commissione UE ai fini dell'adeguatezza. L'interessato può presentare, tramite la propria Autorità indipendente, reclamo al *Civil Liberties Protection Officer*, ma prima ancora l'interessato deve mostrare la propria intenzione di presentare reclamo all'autorità di controllo dello Stato membro dell'UE competente per la vigilanza in merito al trattamento. L'*Officer* a cui viene presentato la prima istanza rientra nell'ambito dell'organo che coordina e supervisiona l'intera comunità di intelligence statunitense, che deve garantire che la sicurezza nazionale avvenga secondo il principio di necessità e proporzionalità, come richiesto dall'*Executive Order* 14086[39]. A seguito della pronuncia del *Civil Liberties Protection*

[39] Si intende far riferimento al *Office of Director of National Intelligence* (ODNI).

Officer ciascun reclamante, nonché ciascun servizio della comunità di intelligence, può chiedere il riesame della decisione dell'addetto alla tutela della vita privata e delle libertà civili dinanzi al *Data Protection Review Court*[40] entro sessanta giorni dalla notifica della decisione del *Civil Liberties Protection Officer*.

È possibile, in alternativa, ricorrere a procedure arbitrali, regolate da norme concordate dal Dipartimento del Commercio e dalla *Federal Trade Commission*, sulla base delle quali la composizione arbitrale di tre arbitri scelti dalle parti, è individuata tra la rosa di una lista di almeno dieci arbitri indicati da Dipartimento del Commercio e dalla Commissione. In tal caso, l'interessato può essere assistito dalla propria autorità nazionale di protezione dei dati per la preparazione del caso da sottoporre al collegio e la decisione di quest'ultimo può essere sottoposta a riesame ai sensi della legge federale sull'arbitrato, ossia attraverso un'istanza presentata al giudice distrettuale federale con competenza territoriale sulla base del luogo in cui si trova il principale centro operativo dell'organizzazione che partecipa al regime.

6. La istituzione di organi preposti al controllo di requisiti e condizioni per garantire un trattamento di dati trasferiti verso gli Stati Uniti, adeguato al GDPR, è sicuramente stato un risultato significativo che manifesta la volontà di rendere efficace le dichiarazioni di principio contenute soprattutto nella recente decisione di adeguatezza. Tuttavia, taluni prerequisiti, come la necessità di essere un'organizzazione che rientri all'interno del perimetro delle attività controllate dal Dipartimento di Commercio e dalla *Federal Trade Commission*, così come le procedure di verifica e "ricertificazione" annuale rendono il *Data Privacy Framework* poco operativo rispetto alle altre modalità individuate dagli artt. 46 e ss del GDPR. Si intende in particolare riferirsi alle clau-

[40] È un tribunale indipendente istituito dal Procuratore generale sulla base del decreto presidenziale 14086, composto da sei giudici, nominati dal Procuratore generale in consultazione con il segretario del commercio e il direttore dell'intelligenza nazionale. I criteri di valutazione sono analoghi a quelli utilizzati per valutare le candidature dei magistrati federali, in considerazioni anche delle maturate esperienze, che non escludono la necessità che i giudici dispongano di un nulla osta di sicurezza per poter accedere a informazioni classificate in materia di sicurezza nazionale.

sole contrattuali tipo, che si presentano maggiormente predisposte a calibrare le specifiche esigenze delle parti perché strutturate in funzione delle peculiarità del caso, ossia dei dati e delle finalità che devono essere perseguite. Un fattore limitante è anche l'assenza di una disciplina federale uniforme sulla tutela dei dati, e la presenza di numerose normative, come quelle sulla sicurezza, che mantengono una posizione prevalente e di riferimento, orientando e condizionando tutte le altre discipline settoriali, che interferiscono con la tutela dei dati. D'altronde, la protezione dei dati è ancora prevalentemente ancorata all'articolo IV della Costituzione americana, ossia al diritto alla privacy in rapporto con il divieto di perquisizioni. Le leggi sulla sicurezza mantengono pertanto la loro posizione di asse ordinante la disciplina dei dati, indirizzandola e limitandone talvolta la tutela complessiva.

La necessità però di conferire centralità ed autonomia al tema della protezione dei dati in una legge federale in grado di creare una base comune è avvertita e comprovata dal disegno di legge (H.R. 8152), proposto nel 2022, noto come *American Data Privacy and Protection Act* (ADPPA)[41] che rivela l'obiettivo di predisporre un apparato normativo idoneo a disciplinare le modalità e le condizioni che devono essere adottate da tutte le imprese, organizzazioni, enti non profit, interessati a raccogliere, trattare, trasferire dati che possono essere identificativi della relazione con le persone fisiche. La proposta non è stata approvata e la scadenza della legislatura durante la quale è stata presentata richiede una nuova formulazione e preclude una sua riproposizione. Tuttavia, è interessante riferire in merito a taluni aspetti di questa proposta, come al concetto di "trasferimento" indicato, che è inteso in senso ampio, ovvero intrinsecamente comprensivo anche della divulgazione del dato da un soggetto all'altro, vale a dire del successivo trasferimento a terzi, purché quest'ultimo compiuto a condizioni però stringenti. La proposta ripercorre in gran parte i punti chiave del regolamento europeo; ne

[41] La proposta ha avuto un sostegno bipartisan ma lo stato della California ha sollevato molte critiche perché in contrasto con il proprio sistema interno statale, invero maggiormente garante di tutele rispetto all'ADPPA. Oltre a vanificare l'evoluzione della normativa statale, la proposta limitava la capacità degli Stati di innovare in materia di diritti digitali, sottraendo poteri all'autorità indipendente californiana, deputata alla tutela dei dati.

consegue che specifica considerazione è rivolta alle imprese, tenute ad applicare il principio della limitazione della raccolta dati affinché essa sia "ragionevolmente necessaria e proporzionata" ai leciti obiettivi che devono essere raggiunti, nonché particolare rilievo è mostrato ai diritti degli individui, soprattutto nella veste di consumatori, che devono essere sempre padroni dei propri dati e a tal fine, vengono introdotti i diritti di accesso dei propri dati, il diritto di correzione e il diritto di cancellazione. L'implementazione di misure di sicurezza e i meccanismi di enforcement vengono affidati alla *Federal Trade Commission* e ai procuratori statali che continuano a mantenere una posizione centrale nel controllo. Inoltre, un trattamento differenziato è proposto a seconda che si tratti di categorie di dati sensibili, cc.dd. *sensitive covered data* con la necessità di un esplicito consenso per i dati di minori o di grandi entità di dati detenuti da grandi entità.

Il GDPR si rivela quindi non solo quale parametro di riferimento per un possibile e lecito trasferimento dati europei verso paesi extra europei, ma anche quale modello guida per tutti gli stati della confederazione[42].

[42] Tra gli Stati che hanno adottato leggi in tema di protezione dei dati e tutela della privacy, tutte entrate in vigore negli ultimi tre anni, è possibile riferire: la Virginia (*Virginia Consumer Data Protection Act - 2023*), il Colorado (*Colorado Privacy Act - 2023*) che tutela in particolare i diritti dei consumatori sul trattamento dei propri dati, il Connecticut (*Personal Data Privacy and Online Monitoring Act - 2023*), Texas (*Texas Data Privacy and Security Act - 2024*) e Oregon (*Oregon Consumer Privacy Act - 2024*). Delaware (*Delaware Personal Data Privacy Act - 2025*), Iowa (*Iowa Consumer Data Protection Act - 2023*), Montana (*Montana Consumer Data Privacy Act - 2024*), New Hampshire (*New Hampshire Data Privacy Act - 2025*) e New Jersey (*New Jersey Data Privacy Act - 2025*). Tutti gli Stati offrono una tutela di grado inferiore rispetto a quella prevista dallo Stato della California e offrono una normativa complessivamente frammentata.

Ad ogni modo, il GDPR rappresenta un'ispirazione per tutti gli Stati, anche non appartenenti alla Confederazione degli Sati Uniti, in ragione anche della singolarità ed ampiezza della normativa, Tuttavia, tutti gli Stati che intendono munirsi di una regolamentazione interna. Tuttavia, gran parte dei recenti framework nazionali realizzati, come in Brasile, in India e in Canada, si basano prevalentemente sull'obbligo di localizzazione dei dati, obbligo che impone di conservare o trattare i dati personali o aziendali all'interno del proprio paese, salvo che siano archiviati, copiati o gestiti su server situati fisicamente nel paese che emette il mandato. Vengono in modo evidente adottate politiche di sovranità digitale, protese ad un controllo sui dati dei propri cittadini e invero poco favorevoli e fiduciose in una sicura condivisione di

Lo scenario di una riforma federale è ancora quindi aperto e si mostra alquanto complesso in ragione delle rivendicazioni dello stato della California che notoriamente rappresenta un laboratorio normativo molto avanzato sul tema del digitale e sulla tutela dei diritti. La normativa californiana, pur non configurando un regime specifico di restrizione ai trasferimenti internazionali, presenta articolate disposizioni che offrono un sistema di tutele più elevato rispetto alla proposta di riforma bocciata, nonché rispetto alle leggi adottate dagli altri Stati. La recente legge, *California Privacy Rights Act* (CPRA), datata 2023, ha modificato ed ampliato la portata del *California Consumer Privacy Act* (CCPA) legge che ha regolato gli aspetti relativi al trasferimento e alla condivisione di dati. Il trasferimento però è subordinato ad obblighi contrattuali stringenti e, sebbene sia introdotta la configurazione di figure analoghe al *service provider* e al *contractor*, il titolare rimane il centro di imputazione della responsabilità del trasferimento.

L'adozione di una disciplina federale neutralizzerebbe la legge californiana e tutte le leggi statali emanate nel settore anche se più garanti della tutela dei dati, ma consentirebbe all'Europa di avere un inter-

dati. Questo approccio comporta sul piano operativo la necessità delle aziende di creare data server locali o spostare server, oppure, se usano iCloud, di affidarsi a provider che garantiscono hosting nel Paese richiesto (a titolo esemplificativo, in Italia, in Germania ed India opera AWS e Azure). Questa gestione comporta dei costi aggiuntivi non da sottovalutare giacché la duplicazione dei sistemi, la costituzione o l'affitto di server nazionali sono attività molto dispendiose, senza considerare le spese dovute alle consulenze legali e le attività di compliance che implicano procedure di audit e certificazioni e investigazioni di esperti preparati a livello internazionale. L'obbligo della localizzazione oltre ad essere onerosa e macchinosa causa delle limitazioni tecniche versus una flessibilità che potrebbe essere offerta da backup internazionali, analisi centralizzata, machine learning), causa al servizio offerto enormi rallentamenti che si amplificano qualora venga intrapresa una verifica giudiziaria che richiede il coinvolgimento di diverse giurisdizioni. Vi sono però anche ordinamenti in fase di grande evoluzione in cui la c.d. *data localization* non è generalizzata ma solo mirata, ossia è richiesta unicamente per alcuni tipi di dato, o quando si tratta di alcuni soggetti e soltanto se sia opportuna per motivi di sicurezza nazionale, interesse pubblico o diritti individuali. Si v. l'esperienza cinese, basata su tre pilastri: la *Cybersecurity Law* (2017), la *Data Security Law*, 2021 e il *Personal Information Protection* (2021). Si v. *Cross-border Data Transfer Regulation in China*, in *Riv. italiana di informatica e diritto*, 2021, 6, vol. 3, p. 69 ss. Cfr. Sahar Iqbal, *Cross-Border Data Transfers and Privacy Regulations: The future of the GDPR and Beyond*, in *Business, Law International*, 2025, Vol. 26, n. 3, p. 217 ss.

locutore senza ombre. Parte integrante dell'efficacia continua dell'adeguatezza sono i controlli periodici che devono essere adottati dalla Commissione per verificare l'effettiva attuazione delle condizioni che avevano portato alla sua adozione, posto che la Commissione, ai sensi dell'art. 45, può rivedere, sospendere o revocare la decisione di adeguatezza in qualunque momento, quando ritenga che non sia più garantito un livello di protezione adeguato. Nell'ottobre 2024 è stato pubblicato il primo rapporto di monitoraggio che, sebbene abbia rilevato l'istituzione da parte degli Stati Uniti delle strutture e dei meccanismi necessari, sembra non ravvedere un concreto successo operativo della decisione, anche in ragione del moderato numero di autocertificazioni registrate e dell'ancor più misurato numero delle imprese che hanno provveduto a rinnovare l'autocertificazione.

La decisione di adeguatezza ad oggi si rivela così non molto adoperata e di certo subisce gli effetti pregiudizievoli legati all'assenza di una invece auspicabile legge federale che ovvierebbe i rischi di interferenze derivanti dall'applicazione di leggi statali eterogenee o di disposizioni in materia di sicurezza, che ad oggi ne compromettono e spesso svuotano l'efficacia e l'applicazione. Queste scelte mostrano come il percorso per un'uniformità di vedute, premessa per una regolamentazione condivisa, si mostra alquanto complesso e ancora non prossimo. In attesa dell'approvazione di una legge federale, le misure alternative, come in particolare le clausole contrattuali tipo sembrano le più idonee ad evitare le esposizioni ai rischi connessi a mutamenti politici, revisioni normative e giudiziarie, che rappresentano le maggiori cause di instabilità nei trasferimenti dati. L'adozione di tali clausole impone al destinatario negli US l'assunzione diretta di responsabilità legali verso l'esportatore UE, in ragione della obbligata personalizzazione del trattamento che esse impongono. Questa prassi sembra così mettere in crisi l'opportunità di investire sulla creazione di procedure che rafforzino l'efficacia di questa dichiarazione di adeguatezza, poiché gli attuali pilastri del sistema federale ne limitano la realizzabilità. L'invito che si palesa sembra dunque quello di percorrere in via prioritaria altre strade di maggiore portata applicativa, in grado di coinvolgere più imprese e organizzazioni, caratterizzate da procedure più snelle sul piano burocratico, come le clausole contrattuali tipo.

DIRITTO ALLA RISERVATEZZA E DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI NELLA SANITÀ DIGITALE. IL CASO DELLA TELEMEDICINA

Livia Saporito

Sommario: 1. Le nuove frontiere della scienza medica: *patient empowerment* e Medicina 4.0. – 2. La telemedicina tra innovazione e regolamentazione. – 3. Il diritto alla riservatezza e il diritto alla protezione dei dati sanitari nell'*e-Health*. GDPR e HIPAA a confronto. – 4. (Dis-)umanesimo digitale e convergenza dei modelli.

1. Nell'opera *Naturalis Historia*[1], Plinio il Vecchio narra di come Catone volesse dissuadere il figlio Marco dal servirsi di medici inviati dalla Grecia per corrompere con la loro "scienza", e sterminare, carpendone la fiducia, il barbaro popolo romano. Quella di Plinio non era una condanna alla medicina in sé, ma all'esercizio della professione medica, rea di generare arricchimento – la professione è stata disciplinata sin dal III secolo a.C. mercè accordi di locazione ed appositi testi giuridici – attraverso i mali della vita umana. Per Celso (*De Medicina*)[2], la *prudentia* è l'indispensabile attributo della professione. Il medico è responsabile ogni qual volta la eserciti con imperizia e negligenza, ad esempio se genera false speranze o omette di dire la verità.

Negli antichi testi latini riecheggia una antica, e mai del tutto risolta, tensione: il medico è colui al quale ci si rivolge speranzosi in una

[1] Plinio il Vecchio, *Naturalis historia*, XX1X, pp. 1-27. Nel proemio, l'Autore delinea una sintetica storia della medicina, dalla quale emerge l'ostilità nei confronti dei medici della sua epoca, sia per motivazioni moralistiche (condanna l'esercizio della professione medica volto ad accumulare denaro), sia per scetticismo sulla fondatezza della scienza medica. Questo orientamento lo porta a rivalutare la posizione di Catone il Censore, che nel II secolo a.C., nell'ambito della sua opposizione alla cultura greca, aveva preso di mira i medici greci attivi a Roma.

[2] Il trattato di Aulo Cornelio Celso, *De Medicina*, p. 3 presenta molte affinità con la ricostruzione di Plinio il Vecchio, probabilmente perché ambedue gli autori utilizzavano le perdute *Disciplinae* di Varrone.

cura, confidando nella guarigione o almeno nella possibilità di poter allungare la propria vita. Speranze che l'avvento delle tecnoscienze e l'utilizzo di strumenti di intelligenza artificiale hanno alimentato, innovando le modalità assistenziali, diagnostiche, terapeutiche e chirurgiche; aprendo a possibilità di cura un tempo inimmaginabili; riducendo, talvolta quasi azzerando, i margini di errore.

La medicina sta vivendo una quarta stagione, cd. Medicina 4.0, ultima in ordine temporale dopo la Medicina 1.0, ovvero la medicina tradizionale che per centinaia di anni si è basata sulle competenze di medici, i quali disponevano di poco più dei cinque sensi per diagnosticare malattie e di un ristretto numero di farmaci, per lo più ricavati da sostanze presenti in natura; la Medicina 2.0, novecentesca, le cui principali innovazioni sono state l'introduzione dei raggi X in campo diagnostico e degli antibiotici in campo terapeutico; la Medicina 3.0, caratterizzata dall'utilizzo di microsistemi e dall'elettronica (chirurgia computer-assistita, riconoscimento d'immagini, robotica).

La Medicina 4.0[3] può essere considerata il corrispettivo, nella scienza e nella pratica medica, della Quarta Rivoluzione industriale[4], e si caratterizza per la fusione di tecnologie fisiche, digitali e biologiche – I.A., *big data*, *Internet of Medical Things*, genomica e medicina di precisione, telemedicina e realtà aumentata, - al fine di sostituire la medicina cd. "di popolazione", basata su medie statistiche, con una medicina (personalizzata, predittiva e preventiva), nella quale il paziente è al centro di un ecosistema interconnesso. Secondo il modello esplicativo delle "4 P", trattasi di una medicina predittiva, capace di individuare il rischio di sviluppare una patologia prima che compaiano i sintomi; preventiva, che agisce in anticipo per evitare l'insorgenza della malattia; persona-

[3] B. Santiago de Mendonça - L.F. Rodrigues - K. Araújo Ferreira, *Healthcare 4.0: a systematic literature review*, in *Journal of Health Organization and Management*, 2025; E. Pasero, *Medicine 4.0: When New Technologies Work with Artificial Intelligence*, in *Instrumentation & Measurement Magazine*, 2024; G. Natale, *L'intelligenza artificiale in sanità. Il dialogo necessario tra medicina, etica e diritto*, Cedam/Wolters Kluwer, 2025.

[4] Il fondatore del World Economic Forum K. Shwab, *The Fourth Industrial Revolution*, Portfolio Penguin, 2016, utilizza questa locuzione per descrivere l'impatto prodotto dall'utilizzo dei dati, dalla digitalizzazione e dall'interazione uomo macchina sulle discipline economiche ed industriali.

lizzata[5], in grado di calibrare la terapia sulle caratteristiche biologiche del singolo individuo; partecipativa, nella quale il paziente ha un ruolo attivo, monitora i propri dati ed è più consapevole del proprio percorso di cura.

In questa prospettiva, l'analisi di enormi quantità di informazioni (cartelle cliniche, stili di vita, genetica) permette all'IA di identificare patterns invisibili all'occhio umano, supportando i medici nella diagnosi precoce e nella scelta della terapia più efficace. Dispositivi indossabili come smartwatch e sensori impiantabili monitorano i parametri vitali del paziente in tempo reale, inviando alert automatici alle strutture sanitarie in caso di anomalie. Il sequenziamento del DNA a basso costo consente di elaborare cure "su misura", basate sul profilo genetico individuale, e di prevedere la predisposizione a determinate malattie o la risposta ai farmaci. La possibilità di effettuare visite a distanza permette di abbattere le barriere fisiche, mentre l'uso della realtà aumentata agevola la pianificazione di interventi chirurgici complessi e la riabilitazione.

Il contenitore tecnologico che permette alla medicina moderna di funzionare è l'*e-Health*[6], espressione che sintetizza l'uso combinato delle tecnologie dell'informazione e della comunicazione (ICT) in ambito sanitario. Nell'ottica del "patient empowerment", le piattaforme di *e-health* ravvisano nel principio di autodeterminazione il fulcro di una

[5] La medicina di precisione tende al trattamento e alla prevenzione delle malattie sulla base della variabilità individuale dei geni, ambiente e stili di vita (personalizzazione) e si basa sulla comprensione deterministica delle malattie, diagnosi di fattori causali, abilità di trattare le cause profonde della malattia, utilizzando strumenti come i database biologici genomici e post-genomici, metodi di caratterizzazione quali "omiche", analisi cellulari e tecnologia "mobile", e la bioinformatica. Le armi principali sono l'immunoterapia e la nanomedicina.

[6] Ad avviso di G. Eisenbach, *What is e-Health*, in *Journal Medicine Internet Research*, 2001, dietro la "e" di "e-Health" si individuano i seguenti concetti: 1) Efficiency; 2) Enhancing quality; 3) Evidence based; 4) Empowerment; 5) Encouragement; 6) Education; 7) Enabling; 8) Extending; 9) Ethics; 10) Equity. In argomento cfr. L. Rufo, *L'intelligenza artificiale in sanità: tra prospettive e nuovi diritti*, *in Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, a cura di D'Aloia, Franco Angeli, 2020, p. 459 ss.; A. Spina, *La medicina degli algoritmi*, in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di F. Pizzetti, Giappichelli, 2018, p. 319 s.

infrastruttura tarata sulle specifiche esigenze del paziente, al quale compete in ultima analisi la scelta in ordine a quali informazioni immettere nel sistema, ai livelli di condivisione e alle applicazioni gestite dalla stessa piattaforma[7].

La cd. sanità elettronica abbraccia la telemedicina (consultazioni a distanza e monitoraggio dei pazienti via video), le app per la salute (monitoraggio della frequenza cardiaca), i dispositivi indossabili (*wearables devices*), la condivisione di dati medici elettronici per diagnosi, trattamento e prevenzione (es. cartelle elettroniche) e l'utilizzo di dispositivi intelligenti medici. Il settore medico sanitario è a livello internazionale quello maggiormente investito dall'automazione e dall'I.A., preceduto solo dalle telecomunicazioni[8]. La *healthcare industry* fa registrare un aumento esponenziale (circa 87%) dell'utilizzo di dispositivi intelligenti ed il trend sembra destinato a crescere.

Nonostante gli indubbi benefici in termini di maggiore efficienza, riduzione dei costi e migliori cure attraverso l'impiego di una minore quota di personale sanitario, siffatta evoluzione della scienza medica solleva questioni giuridiche complesse, soprattutto in termini di *privacy*, sicurezza e responsabilità medica, oltre ad interrogativi di ordine etico - l'uso degli algoritmi nelle decisioni cliniche reca con sé il rischio di "deumanizzare" il rapporto medico-paziente e di escludere i soggetti privi di competenze digitali o di accesso a una connessione internet (cd. *digital divide*) – e squisitamente tecnico, come la interoperabilità, la necessità cioè che sistemi informatici diversi (di ospedali o regioni differenti) riescano a comunicare tra loro senza intoppi. A ciò si aggiunga che, a fronte dell'utilizzo delle nuove tecnologie, il paziente nutre, sul

[7] Per P. Guarda, in P. Guarda - G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023, p. 298, «le piattaforme di e-health inducono a concepire l'intera infrastruttura non solo in base alle esigenze professionali o manageriali dei titolari del trattamento, ma in misura crescente alla luce degli interessi di cui il paziente è portatore. Il principio di autodeterminazione altro non è che lo strumento che permette di dare contenuto giuridico a tali esigenze».

[8] Secondo B. Siwicki, *86% of Healthcare Companies Use Some Form of AI*, 19 maggio 2017, consultabile all'indirizzo: www.healthcareit-news.com, «about 86 percent of healthcare provider organizations, life science companies and technology vendors are currently using artificial intelligence technology».

piano psicologico, aspettative ancor più elevate nei confronti della medicina; sviluppa un sentimento di rifiuto rispetto ad eventi avversi ed esiti infausti della patologia; esige di poter far affidamento su di un corpus di regole di responsabilità atte a scoraggiare (*deterrence*) e, se del caso, sanzionare condotte di *medical malpractice*; reclama con forza la riparazione della lesione eventualmente patita. Dall'altra parte, il professionista - cui si richiede ben più di un gesto terapeutico, del saper fare, bensì un "sapere", vale a dire la capacità di orientarsi in un quadro sistemico di spiegazione e di interpretazione dei casi del suo "oggetto-soggetto", l'uomo – dalle stesse regole si attende che non producano l'indesiderabile effetto della *overcompensation*, vale a dire l'esponenziale aumento del contenzioso giudiziario e delle richieste di risarcimento di danno, principale causa della *overdeterrence*[9] della classe medica e delle strutture ospedaliere (e, di riflesso, delle compagnie di assicurazione), pronte ad azionare il meccanismo della medicina difensiva (abbandono delle specializzazioni più a rischio; ricorso ad esami diagnostici superflui prima di ogni intervento).

2. Uno dei pilastri della Medicina 4.0 è la telemedicina[10], strumento che utilizza il quadro tecnologico composto da IA, *big data* e sensori per erogare cure a distanza a vantaggio della collettività.

Nella visione 4.0, la salute non è più confinata tra le mura di un ospedale, ma diventa ubiqua e raggiunge il paziente ovunque egli si

[9] Su questi profili si sofferma Corte Costituzionale n. 178 del 14.05.2010, a cui avviso i fenomeni della *overdeterrence* e della *overcompensation* spingono verso la conciliazione stragiudiziale delle controversie per danni derivanti da prestazioni sanitarie.

[10] Le Linee guida ministeriali del 2014 definiscono la telemedicina «una modalità di erogazione dei sevizi di assistenza sanitaria, tramite il ricorso a tecnologie innovative, in particolare alle Information and Communication Technologies, in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località». Tale definizione va integrata con le previsioni di cui alle successive "Linee guida organizzative contenenti il modello digitale per l'attuazione dell'assistenza domiciliare", approvate con Decreto del Ministro della salute del 29 aprile 2022, a corredo del PNRR (in argomento cfr. N. Posteraro, *La telemedicina*, in V. Bontempi, *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, Roma Tre Press, 2022, p. 201 ss., e con riferimento specifico alle cure in risposta all'emergenza pandemica, *L'assistenza domiciliare integrata* a cura di M.A. Sandulli, Editoriale scientifica, 2021).

trovi attraverso tre modalità principali: la televisita, il telemonitoraggio e la teleassistenza. Nel primo caso, che costituisce l'evoluzione digitale della visita tradizionale, medico e paziente - o anche due medici tra loro (teleconsulto[11]) - interagiscono in tempo reale tramite video-conferenza. La televisita è indicata soprattutto per controlli di pazienti già valutati di persona. Nel telemonitoraggio, che è il nucleo della Medicina 4.0, grazie ai sensori IoMT, come smartwatch o patch cutanei, i parametri vitali - ad esempio pressione, saturazione, glicemia - e i sintomi di un paziente vengono analizzati dall'intelligenza artificiale e segnalati al medico solo se trattasi di casi meritevoli di attenzione. La teleassistenza, infine, è un'attività svolta da personale sanitario (es. infermieri) per supportare a distanza il paziente nella gestione della malattia, nella riabilitazione o nel follow-up terapeutico, soprattutto ove si tratti di soggetti fragili o anziani, con difficoltà negli spostamenti fisici.

Rispetto ai primordi della "vecchia" telemedicina[12], la quale si caratterizzava per realizzare una connessione tra medico e paziente attraverso una semplice telefonata o una videochiamata, oggi ci si avvale di dispositivi IoT interconnessi in tempo reale, che consentono al personale medico di analizzare in prima persona, con il mero supporto di algoritmi predittivi, un consistente e continuo flusso di dati, sulla base dei quali è fornita la diagnosi o la cura. Sostituendo la presenza fisica e curando i pazienti direttamente a casa propria, la telemedicina si propone di

[11] Il teleconsulto consente la collaborazione a distanza tra due o più medici per discutere la situazione clinica di un paziente, scambiando dati e referti, senza la presenza del paziente.

[12] L'Organizzazione Mondiale della Sanità (OMS) definisce la telemedicina nei seguenti termini: «the delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities». Per un inquadramento della materia cfr., nella vasta bibliografia sul tema, A. Pisani, *Telemedicina: quadro normativo, tutele e diritti, sistema delle responsabilità*, Bologna University Press, 2024; V. Molaschi, *Telemedicine: Impact and Perspectives in Healthcare Delivery and Organization of the Italian National Health Service*, in *European Review of Digital Administration & Law*, 2023. In prospettiva europea e comparata v. *Telemedicine*, a cura di D. W. Ford - S.R. Valenta, Springer, 2021; B. Stanberry, *Legal and ethical aspects of telemedicine*, in *Journal of Telemedicine and Telecare*, 2021.

favorire la de-ospedalizzazione, con conseguente riduzione dei rischi di infezioni nosocomiali ed abbattimento dei costi; di garantire continuità assistenziale attraverso un monitoraggio costante, non più cadenzato nel tempo (ad esempio la visita ogni sei mesi); di rendere accessibili i consulti con i migliori specialisti anche a chi vive in zone remote, e di prevenire l'insorgenza di malattie, in luogo di curarne meramente i sintomi. La telemedicina ha l'obiettivo di migliorare l'accesso, l'efficienza e la qualità delle cure, eliminando le barriere geografiche e offrendo uno strumento – che non è una alternativa alla medicina tradizionale[13] - qualora le visite in presenza non siano possibili o necessarie.

In questa prospettiva, diremmo preventiva e proattiva, tale pratica diviene il braccio operativo della medicina intelligente, nella quale il paziente non è più utente passivo del servizio, ma diviene parte attiva di un processo che lo vede protagonista. Nondimeno, l'integrazione dell'IA nei dispositivi medici digitali e negli strumenti diagnostici rappresenta la sfida più avanzata per la tutela della *privacy*[14], che, nel contesto dell'*e-Health*, assume una triplice significazione, rilevando, in senso tradizionale, come esigenza di protezione avverso potenziali violazioni del diritto di ciascuno al rispetto della vita privata e familiare, e, all'indomani dell'entrata in vigore della Carta di Nizza, quale diritto alla protezione dei dati personali[15] (art.7); nonché in relazione al concetto di confidenzialità, principio fondamentale in ambito sanitario che evoca - come recita il giuramento di Ippocrate[16] - la solennità del segreto medico.

[13] «La telemedicina non costituisce un trattamento alternativo, atto a sostituire la tradizionale relazione medico-paziente, bensì consiste in uno strumento che va a potenziare l'erogazione della prestazione sanitaria, cercando di ridurre i limiti legati alla distanza tra i soggetti coinvolti» (testualmente P. Guarda - G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, cit., p. 308 s.).

[14] L. Zambelli, *Telemedicina e privacy: profili oggettivi in ambito sanitario e medico-sportivo*, Università di Bologna, 2023.

[15] Il regime giuridico che regola il trattamento dei dati personali a livello europeo è ora espressione dell'articolo 8 della Carta dei diritti fondamentali dell'UE, che riconosce la protezione dei dati personali come diritto fondamentale e autonomo rispetto alla protezione della vita privata (art. 7).

[16] «Ciò che io possa vedere o sentire durante il mio esercizio o anche fuori dell'esercizio sulla vita degli uomini, tacerò ciò che non è necessario sia divulgato, ritenendo come un segreto cose simili».

Sebbene si tratti di nozioni interdipendenti, la *privacy* è, a rigore, il diritto di un individuo di essere lasciato solo e di esercitare il controllo su come le proprie informazioni personali sono raccolte, utilizzate e condivise; là dove la confidenzialità si riferisce al dovere che incombe sul sanitario (medico, infermiere, ospedale) di proteggere le informazioni affidategli e di non divulgarle senza autorizzazione. Il rapporto tra *privacy* e sanità digitale è un'area di continua tensione normativa, nella quale la velocità della rivoluzione tecnologica mette costantemente alla prova la capacità del diritto di tutelare il paziente. Ne è riprova il fatto che il recente *AI Act*[17] classifica i sistemi di intelligenza artificiale destinati a scopi medici come "ad alto rischio", imponendo rigorosi requisiti di governance dei dati, supervisione umana e robustezza del sistema.

Nei sistemi giuridici europei, la complessità della materia è accresciuta dalle stringenti prescrizioni del Regolamento Generale sulla Protezione dei Dati[18], il quale, nel considerare i dati relativi alla salute fisica e mentale (art. 4) come una delle categorie più delicate di informazioni personali, meritevoli di una speciale protezione, rende ardua la ricerca di un ragionevole punto di equilibrio tra innovazione e regolamentazione. Il GDPR stabilisce, infatti, il generale divieto di trattare i dati sanitari (art. 9, par. 1), salvo casi eccezionali in cui il trattamento appaia necessario per la diagnosi, la prestazione di assistenza o la terapia sanitaria (art. 9, par. 2, lett. h) o per motivi di interesse pubblico rilevante, come la sanità pubblica e la ricerca (art. 9, par. 2, lett. g). L'enorme mole di informazioni relative alla salute dell'uomo indispensabile per addestrare le macchine intelligenti contrasta, inoltre, con il fondamen-

[17] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Legge sull'intelligenza artificiale).

[18] Il Regolamento Generale sulla Protezione dei Dati (GDPR-Reg. UE 2016/679) rappresenta la normativa cardine in Italia e in Europa. L'art. 9 stabilisce il divieto generale di trattare dati sanitari, con eccezioni tassative.

L'uso della telemedicina richiede l'applicazione rigorosa del Regolamento Generale sulla Protezione dei Dati (GDPR - Regolamento UE 2016/679) e della normativa nazionale (come il Codice della Privacy).

tale principio di minimizzazione, che impone l'impiego solo dei dati strettamente necessari. Ancora, il diritto ad essere informati (art. 22 GDPR) sulle decisioni automatizzate mal si concilia con l'opacità - il cd. effetto *black box*[19]– e con la mancanza di trasparenza[20] che connotano i processi decisionali dei software, rendendo di fatto impossibile al paziente la contestazione di una diagnosi o di una decisione terapeutica basata sull'IA.

Nel caso della telemedicina, diritto alla riservatezza, diritto alla protezione dei dati personali e confidenzialità assumono una portata rinforzata, amplificando le difficoltà di operare un bilanciamento tra interessi confliggenti[21]. Da una parte v'è l'interesse del paziente all'efficacia della cura in termini di velocità ed accessibilità, dall'altra l'esigenza di tutela della sua *privacy*, ampiamente intesa. In particolare, per un verso, occorre garantire, il diritto del paziente a stabilire chi può accedere ai propri dati e per quale scopo (cd. autodeterminazione informativa); per altro verso, sussiste l'obbligo del professionista e/o della struttura sanitaria di mantenere segrete le informazioni, mettendole a disposizione unicamente di chi sia specificamente autorizzato (*need-to-know*); nonché di predisporre misure tecniche e organizzative - crittografia, *firewall*, autenticazione -, atte a garantire la protezione e l'integrità dei dati, previa individuazione dei rischi connessi al servizio (cd. valutazione d'impatto sulla protezione dei dati).

Contrariamente alla regola, qui il consenso del paziente non si limita all'atto medico, ma deve riguardare l'utilizzo specifico della tec-

[19] W.N. Price, *Black-box Medicine*, in *Harward Journal of Law & Technology*, 2015, p. 419 ss.; K. Karaboue, *Intelligenza artificiale nell'ambito del sistema sanitario. Implicazioni in termini di privacy alla luce del nuovo GDPR*, in *Amministrativamente*, I, 2023, p. 359 ss.; J. Burrell, *How the Machine "Thinks": Understanding Opacity in MachineLearning Algorithms*, in *Big Data & Soc'Y*, 2016, vol. 3, p. 1 ss.

[20] La segretezza degli algoritmi, intesa come impossibilità di conoscere le modalità del loro funzionamento, è ad avviso S. Rodotà, *Il diritto di avere diritti*, Laterza, 2012, p. 462, il contraltare della maggiore trasparenza e dei maggiori controlli di cui beneficia la società per effetto delle nuove tecnologie.

[21] In argomento cfr. C. Botrugno, *Tecnologie dell'informazione e della comunicazione e tutela della salute: le sfide aperte tra protezione, circolazione e riutilizzo dei dati*, in *Diritto e questioni pubbliche*, XX, 2020, p. 137 ss.; E. Sorrentino - A.F. Spagnuolo, *Dati sanitari: aperti, accessibili e riutilizzabili*, in *MediaLaws*, I, 2022, p. 170 ss.

nologia (es. piattaforma video, sensori)[22], tenuto conto della peculiare modalità di erogazione della prestazione sanitaria a distanza. Oltre all'informativa tradizionale relativa ai rischi ed i benefici della diagnosi e/o della cura, nella telemedicina devono essere esplicitati aspetti tecnici e logistici: il paziente deve essere preventivamente informato circa la tipologia di visita (televisita, teleconsulto o telemonitoraggio) e circa la sicurezza della piattaforma utilizzata (crittografia, server protetti). Occorre un consenso specifico affinché la sessione venga registrata o per acquisire immagini/fermo-immagine.

Invero, in questa pratica medica, la confidenzialità è messa alla prova dalla natura stessa del servizio, che avviene in assenza fisica del professionista e attraverso reti potenzialmente vulnerabili. Le modalità di erogazione a distanza espongono i dati a rischi specifici: durante un teleconsulto video o in occasione dell'invio dei dati del telemonitoraggio la comunicazione può essere intercettata (rischio di attacco "man-in-the-middle"); i dispositivi del paziente, come smartphone, tablet e *wearable device*, o dello stesso professionista, il pc ad esempio, possono favorire fenomeni di *malware* o accessi non autorizzati. Lo stesso è a dirsi ove la piattaforma utilizzata – sovente si fa ricorso a piattaforme di comunicazione generiche (Zoom, Google Meet, ecc.) adattate alla sanità - non sia certificata o gestita con standard di sicurezza adeguati, esponendo i server nei quali sono conservate le registrazioni o le cartelle cliniche elettroniche ad ingressi illegittimi.

Per scongiurare queste eventualità, il personale sanitario è gravato da una serie di obblighi, che vanno dal vincolo, discendente dal codice deontologico, di mantenere il segreto professionale e d'ufficio sulle informazioni apprese durante la cura, alla responsabilità (*accountability*) del professionista o dell'ente sanitario titolare del trattamento, il quale

[22] Il consenso può essere raccolto in diverse modalità, attraverso la firma elettronica (FEA o FEIP) o la pressione di un tasto "accetto" su piattaforme certificate, previo invio dell'informativa, oppure in formato cartaceo, scansionato e trasmesso via email/portale prima della prestazione, purché sia esplicito e documentato. Il paziente ha il diritto di revocare il consenso in qualsiasi momento e di richiedere una visita in presenza, senza che ciò comprometta la continuità delle cure. Per un inquadramento del tema in termini generali v. A. Pioggia, *Consenso informato ai trattamenti sanitari e amministrazione della salute*, in *Riv. trim. dir. pubbl.*, I, 2011, p. 127 ss.

deve dimostrare di aver adottato tutte le misure necessarie per proteggere i dati, inclusa la scelta di piattaforme e fornitori che offrano adeguate garanzie di confidenzialità[23], fino alla documentata designazione del personale legittimato ad accedere ai dati e ai sistemi di telemedicina. In virtù del sopra evocato principio "need to know", l'accesso ai dati sanitari digitali deve essere limitato al personale sanitario direttamente coinvolto nella cura del paziente. I sistemi di telemedicina devono prevedere meccanismi di autenticazione forte e la tracciabilità (*log*) di ogni accesso. Sul piano tecnico è, poi, doverosa, l'adozione di strumenti come la crittografia forte (*end-to-end encryption*) per essere certi che solo il medico e il paziente possano decifrare il contenuto della seduta e di sistemi di autenticazione a più fattori (*multi-factor authentication*) per prevenire l'accesso alle piattaforme con credenziali rubate.

I sistemi devono, inoltre, dotarsi di un registro degli accessi onde stabilire chi, quando e da dove ha avuto accesso a un dato (o a un teleconsulto). Le cartelle cliniche elettroniche e i dati di telemonitoraggio devono, infine, essere consultabili solo tramite autorizzazioni granulari, basate sul ruolo specifico dell'operatore sanitario. In sintesi, assicurare la confidenzialità nella telemedicina significa applicare i principi tradizionali del segreto professionale a un ambiente digitale e interconnesso, utilizzando la sicurezza informatica come strumento imprescindibile per adempiere agli obblighi di legge.

Un ulteriore profilo critico della telemedicina attiene alla proliferazione dei dati ed alla gestione dei metadati. Il telemonitoraggio, in particolare, implica la raccolta continua e massiva di dati da sensori, la quale, se non essenziale, può violare il principio della minimizzazione, fornendo informazioni di carattere non sanitario, come l'orario di accesso, la posizione o l'indirizzo IP, rivelatrici di abitudini e della vita privata del paziente.

La telemedicina, in tutte le sue declinazioni, deve essere supportata da un quadro normativo rigoroso e da soluzioni tecnologiche proget-

[23] Ove ci si avvalga di una piattaforma esterna, l'azienda fornitrice funge da Responsabile del Trattamento (DPO/Processor). È obbligatorio formalizzare un Accordo sulla Responsabilità del Trattamento (DPA) con il fornitore della piattaforma per imporre a quest'ultimo l'adozione degli standard di sicurezza richiesti dal GDPR sui dati sanitari. L'utilizzo di piattaforme non conformi espone a gravi sanzioni.

tate fin dall'inizio per tutelare il dato. La piena fiducia del paziente nella riservatezza e nella protezione dei dati personali è il presupposto indefettibile per l'efficacia e l'accettazione sociale di questo nuovo modello di assistenza che colloca il paziente all'interno di un ecosistema di servizi sanitari avanzati.

3. Il termine *privacy*, come si osservava, comprende sia la dimensione del diritto alla riservatezza, ossia alla protezione della vita privata e familiare, sia il diritto al controllo dei dati personali, sia, infine, la nozione di confidenzialità. La *privacy*, così intesa, è, senza dubbio, la sfida normativa più pressante che si profila nell'ambito dell'*e-Health*. Una sfida nella quale il diritto comparato fornisce un contributo fondamentale per comprendere come i quadri normativi esistenti si adattino alla nuova realtà della sanità digitale, nella ricerca di un ragionevole equilibrio tra innovazione, tutela dei diritti fondamentali e sicurezza dei pazienti.

In questa prospettiva, il confronto tra il modello europeo (GDPR) e quello statunitense (HIPAA) evidenzia filosofie profondamente diverse. Il primo si caratterizza per un approccio proattivo e per la predisposizione di un elevato livello di *privacy* e protezione dei dati personali "by design"[24], fin cioè dalla fase di progettazione; il secondo è, invece, dichiaratamente orientato al mercato e all'operatività del sistema sanitario.

In particolare, il Regolamento Generale sulla Protezione dei Dati stabilisce uno standard rigoroso ed uniforme per il trattamento di tutti i dati personali, inclusi quelli sanitari, con applicazione estesa alle aziende che trattano informazioni relative ai cittadini UE, indipendentemente dalla loro sede (*long arm jurisdiction*), ed impone requisiti particolarmente severi in tema di consenso, minimizzazione dei dati e valutazioni d'impatto. L'UE adotta un approccio orizzontale e basato sui diritti (*principle-based*) e, conformemente alla logica *opt-in* cui è ispirato, postula, ai fini del trattamento dei dati sanitari, un consenso

[24] Sul concetto di "privacy by design", elaborato dalla dottrina canadese ed adottato a livello di policy in altri ordinamenti giuridici, tra cui gli Stati Uniti, cfr. P. Guarda - G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, cit., p. 85.

esplicito, libero, specifico e informato. Attesi la natura sensibile delle informazioni relative alla salute dell'individui e l'uso di nuove tecnologie, il GDPR richiede spesso l'esecuzione di una valutazione d'impatto sulla protezione dei dati (DPIA). Questo è un processo che serve a identificare e mitigare i rischi per i diritti e le libertà degli interessati (i pazienti) derivanti dal trattamento dei dati.

Negli USA, la materia è regolata da una legge federale del 1996, l'*Health Insurance Portability and Accountability Act* (HIPAA)[25], concepita, in origine, come strumento atto a garantire ai lavoratori di mantenere la copertura assicurativa sanitaria anche durante i periodi di transizione, ed oggi considerata la normativa di riferimento per la protezione dei dati sanitari e della *privacy* dei pazienti avverso accessi non autorizzati o fughe di dati[26].

Diversamente dal GDPR, la portata applicativa della legge è settoriale e verticale. Essa riguarda i soli *covered entities*[27] (medici, ospedali, cliniche, assicurazioni) ed i loro associati commerciali (es. fornitori di software di archiviazione, consulenti legali o amministrativi)[28], lasciando potenzialmente non regolamentati i dati raccolti da *wearable devices* o da app per il benessere non direttamente connesse con i fornitori di assistenza sanitaria. L'HIPAA si articola in tre regole fondamentali: la "Privacy Rule", la "Security Rule" e la "Breach Notification Rule". Alla *Privacy Rule* compete l'individuazione delle informazioni protette, la definizione di come e quando le *protected health information* (PHI) possono essere utilizzate o divulgate e l'individuazione dei casi in cui i pazienti hanno il diritto di ottenere copia delle proprie cartelle cliniche.

[25] *Health Insurance Portability and Accountability Act* (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[26] P. Guarda - G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023.

[27] La limitazione ai cc.dd. "enti coperti" segna una sostanziale differenza rispetto al GDPR. Restano sottratti all'applicazione della legge federale sia le app per il benessere, sia i dispositivi indossabili che raccolgono dati sanitari direttamente dagli utenti senza essere associate ad un medico o ad un piano assicurativo, creando il cosiddetto *HIPAA Gap* nella *e-Health*.

[28] Business associates sono entità che gestiscono dati sanitari per conto delle covered entities.

Conformemente al principio del "minimo necessario", *covered entities* e loro associati sono soggetti a rigorosi standard di confidenzialità e sono chiamati a compiere ogni ragionevole sforzo per limitare l'uso, la divulgazione e la richiesta di informazioni protette a quanto strettamente necessario per adempiere allo scopo specifico. I pazienti devono essere informati, attraverso un apposito documento, delle modalità attraverso cui l'ente utilizzerà o divulgherà le informazioni sanitarie, oltre a poter accedere alle proprie PHI e a chiederne la rettifica in caso di errore.

L'approccio permissivo che ispira la legge statunitense è a fondamento della non obbligatorietà dell'autorizzazione[29] scritta del paziente – nozione solo vagamente assimilabile a quella di consenso di cui al GDPR[30] – per l'utilizzo dei propri dati per scopi di cura (*treatment*), ad esempio per finalità di condivisione con specialisti, per l'ottenimento di rimborsi dai piani sanitari (*payment*) o per lo svolgimento di attività amministrative e legali di gestione dell'ente (*healthcare operations*), come nel caso del controllo di qualità o della formazione. L'*authorization* è, invece, richiesta per il conseguimento di finalità diverse, quali il marketing o la ricerca non correlata alle attività che costituiscono il core business del sistema sanitario, riassunte nell'acronimo TPO (*treatment, payment, operations*).

A differenza della *Privacy Rule*, che si applica a tutte le forme di dati (verbali, cartacei, digitali), la *Security Rule* è un framework tecnico-giuridico volto a garantire la confidenzialità, l'integrità e la disponibilità (*confidentiality*, *integrity*, and *availability*) delle informazioni digitali,

[29] L'*authorization* è un documento formale che deve avere una data di scadenza e descrivere esattamente quali informazioni saranno utilizzate e da chi. A differenza del GDPR, una volta che i dati escono dal perimetro delle *covered entities*, ad esempio perché ceduti a un'app di fitness non legata a un medico, l'HIPAA cessa di trovare applicazione.

[30] Per un confronto tra i modelli in tema di consenso cfr. M. Jurczuk - M. Suprunowicz, *Consent in Data Privacy: A General Comparison of GDPR and HIPAA*, Przegląd Prawniczy Uniwersytetu Im. Adam Mickiewicza, 2024, vol. 16, p. 173 ss., le quali evidenziano il minor rigore della legge federale rispetto al sistema "opt-in" del GDPR; e C. J. McKinstry, *The HIPAA Privacy Rule: Flawed Privacy Exposed When Compared with the European Union's General Data Protection Regulation*, in *Journ. of Healthcare Finance*, vol. 45, n. 1, Summer 2018, p. 1 ss., a cui avviso le profonde falle strutturali presenti nell'HIPAA rispetto al modello UE sono responsabili dell'edificazione di un sistema di "riservatezza" piuttosto che di vera privacy.

prevedendo strumenti di protezione di tipo amministrativo (politiche interne e formazione del personale), fisico (sicurezza dei locali e dei dispositivi) e tecnico (sistemi di criptazione, password e controlli d'accesso). La regola rende, in buona sostanza, operativi i principi di riservatezza stabiliti dalla *Privacy Rule*, concentrandosi in via esclusiva sulla protezione dei dati sanitari in formato elettronico (e-PHI) attraverso la predisposizione di misure di salvaguardia ora obbligatorie, ora suscettibili di valutazione da parte dell'ente[31].

In virtù della *Breach Notification Rule*, le strutture sanitarie hanno l'obbligo di notificare[32] l'avvenuta violazione dei dati ai pazienti interessati, al Dipartimento della salute e, nel solo caso in cui l'evento coinvolga più di cinquecento residenti di uno Stato, i media locali. Per violazione si intende l'acquisizione, la consultazione, l'utilizzo o la divulgazione di dati protetti in maniera non conforme alla Privacy Rule. In materia vige una presunzione di colpa: ogni uso non autorizzato è considerato *breach*, a meno che l'organizzazione dimostri, tramite un'analisi dei rischi, che v'è una bassa probabilità che i dati siano stati compromessi.

Tra il 2024 e l'inizio del 2026, l'HIPAA è stato oggetto di significative modifiche con l'intento di garantire la protezione della *privacy* in ambiti particolarmente sensibili e di scongiurare l'aumento dei cyberattacchi. In questa prospettiva si giustifica l'introduzione di una controversa[33] norma, *The Reproductive Health Privacy Final Rule* (2024-2025), che garantisce la riservatezza dei dati relativi alle scelte riproduttive, purché consentite nei singoli stati federati - quali aborto,

[31] La *Security Rule* stabilisce gli standard per proteggere i PHI che sono creati, ricevuti, mantenuti o trasmessi elettronicamente (e-PHI) mediante misure tecniche che obbligano all'implementazione dei meccanismi per proteggere l'accesso e controllare l'integrità dei dati, inclusi crittografia e controlli d'accesso.

[32] La comunicazione agli interessati deve includere una breve descrizione dell'accaduto, la specificazione della tipologia tipi di dati coinvolti (es. nome, codice fiscale, diagnosi), indicazioni ai pazienti al fine di ottenere protezione, informazione circa le misure adottate dagli enti per indagare e mitigare i danni.

[33] Nel giugno 2025, un tribunale federale ha annullato parte di questa norma. Tuttavia, molte organizzazioni sanitarie continuano ad adottare politiche restrittive per proteggere questi dati in attesa di ulteriori sviluppi.

contraccezione o fecondazione assistita -, facendo divieto a medici e compagnie di assicurazione di rivelare informazioni sanitarie per indagare o perseguire penalmente un individuo per il sol fatto di aver cercato, ottenuto o fornito assistenza sanitaria riproduttiva (lecita). La regola si preoccupa, all'indomani dell'*overruling* del caso Roe *v.* Wade (1973) operato dalla Corte Suprema con la sentenza Dobbs *v.* Jackson Women's Health Organization (2022)[34] e dell'emanazione delle cc.dd. "Trigger Laws" - leggi statali sull'aborto approvate anni prima di Dobbs (2022), ma rimaste dormienti perché incostituzionali pendente il precedente Roe *v.* Wade -, di garantire, attraverso il meccanismo della dichiarazione scritta[35], uno scudo legale ai sanitari avverso le richieste delle forze dell'ordine degli Stati dove l'aborto è illegale, volte a cercare prove (cartelle cliniche, dati GPS, messaggi) per perseguire penalmente chi si recava in altri Stati per accedere questa pratica. La *Reproductive Health Care Privacy Rule* costituisce, in buona sostanza, la risposta dell'amministrazione federale all'esigenza di garantire tutela ad una nuova declinazione del fondamentale diritto alla riservatezza[36], relativa alle scelte riproduttive individuali, onde impedire che le strutture diventino, di fatto, informatori della polizia. Il novello quadro normativo ha subito, tuttavia, un contraccolpo durante l'amministrazione Biden

[34] Nel precedente Roe *v.* Wade 410 U.S. 113 (1973), la Corte Suprema USA ha limitato drasticamente il potere degli stati federati di vietare l'interruzione volontaria di gravidanza, facendo leva sulla necessità di preservare il pluralismo ideologico all'interno di una società autenticamente democratica. Nel successivo caso "Dobbs" (19-1392, 597 U.S. del 24 giugno 2022), i giudici federali hanno, con una maggioranza di sei a tre, invece, affermato la legittimità di una legge del Mississippi (*Gestational Age Act*), che vieta l'aborto dopo la quindicesima settimana di gestazione, osservando che la Costituzione degli Stati Uniti non comprende un diritto all'aborto; perciò i singoli stati sono liberi di regolare la materia. Per una attenta ricostruzione della tematica, antecedente al caso Dobbs, cfr. A. Somma, in E. Mostacci - A. Somma, *Gli Stati Uniti e il loro diritto*, Giappichelli, 2023, p. 222 ss.

[35] L'ente sanitario deve ottenere una attestazione scritta dal richiedente, il quale deve confermare che la richiesta non ha lo scopo di investigare o perseguire qualcuno per cure riproduttive lecite.

[36] Per un commento della regola nella specifica prospettiva del rapporto medico-paziente cfr. C. Shachar, *New Reproductive Privacy Rule to Protect Both Patients and Physicians,* 2024, in *JAMA*, August 13, 2024, p. 453 ss.

per effetto di una decisione della *District Court* del Texas,[37] la quale ha, in primo grado, annullato gran parte della previsione normativa, accusando il Dipartimento della salute di aver ecceduto la propria autorità federale[38] e di aver interferito con le leggi statali in materia[39]. La sentenza è stata confermata in appello dalla *Fifth Circuit Court*, nota per essere una delle più conservatrici del paese; conseguentemente le garanzie per la salute riproduttiva introdotte nel 2024 non sono allo stato applicabili, mentre restano in vigore le tutele standard della HIPAA *Privacy Rule* del 2000.

Di analogo tenore, dunque nel segno di un adeguamento degli standard di riservatezza a inedite esigenze di tutela, è la modifica dell'HIPAA nella parte concernente i dati sui disturbi da uso di sostanze che generano dipendenza. I pazienti possono ora firmare un unico consenso per permettere l'uso delle informazioni personali per scopi di

[37] L'amministrazione Biden, tramite il Segretario alla Salute Xavier Becerra, ha emesso linee guida interpretative dell'EMTALA (*Emergency Medical Treatment and Labor Act),* secondo le quali i medici sono obbligati a fornire trattamenti stabilizzanti, incluso l'aborto, ove necessario per salvare la vita o la salute della paziente, prevalendo, se del caso, sulla normativa statale. Il Texas ha fatto causa al governo federale, sostenendo che l'*Act* non autorizza il Governo a praticare interruzioni di gravidanza in violazione delle leggi dei singoli stati federati (in Texas l'aborto è consentito esclusivamente in casi di estremo pericolo di vita, non genericamente per motivi di "salute" della madre). In primo grado, il giudice James Wesley Hendrix ha dato ragione al Texas, assumendo che l'EMTALA è "silente" sul tema dell'aborto e non può essere usato per scavalcare il potere degli stati di regolare tale pratica medica. In appello - Texas v. Becerra No. 23-10246 (5th Cir. 20242024) -, la Corte ha confermato la sentenza di primo grado, osservando che il testo dell'EMTALA non entra in conflitto diretto con il divieto di aborto del Texas, poiché la legge federale richiede di stabilizzare sia la madre che il nascituro («unborn child»).

[38] W.A. Bach - N. Terry, *How Dobbs Threatens Health Privacy*, Harvard Law School (Petrie-Flom Center), 2023/2024 esplorano la nozione di sorveglianza sanitaria post caso "Roe", auspicando leggi federali più stringenti.

[39] Per una analisi del frastagliato quadro legislativo statunitense in tema di salute sessuale e riproduttiva all'indomani del caso Dobbs, cfr. R. Bizzarri, *L'aborto negli Stati Uniti due anni dopo Dobbs v. Jackson Women's Health Organization: sviluppi, dinamiche e prospettive*, in *Osservatorio costituzionale*, 2024, n. 3, p. 304 ss., la quale imputa la disomogeneità normativa alle preferenze politiche dei singoli stati federati, con importanti ricadute in termini di eguaglianza.

trattamento, pagamento e operazioni sanitarie, rendendo la gestione dei dati più simile a quella degli altri dati medici.

È, invece, ancora una mera proposta[40] quella formulata dal Dipartimento della salute volta ad aggiornare la *Security Rule* per far fronte ai massicci attacchi hacker subiti dal sistema sanitario statunitense - come il caso Change Healthcare – attraverso la conversione delle misure di salvaguardia da flessibili in obbligatorie e l'introduzione di strumenti di Multi-Factor Authentication, di richiesta esplicita per i dati sia "in transito" che "at rest", salvati cioè sui server, e di audit annuali a carico delle aziende. Tanto a conferma del fatto che l'attenzione del legislatore (federale) non è rivolta soltanto ad una formale *compliance*, ma anche alle nuove frontiere della sovranità del dato e della cyber-resilienza.

4. La comparazione dei modelli europeo e nordamericano evidenzia, *prima facie*, profonde divergenze di ordine strutturale e funzionale. L'HIPAA è, come si è detto, una legge settoriale, che si applica al solo contesto sanitario ed a specifici soggetti, mentre il GDPR ha una portata universale e si prefigge di proteggere il dato personale in quanto tale. La legge federale si connota per un approccio reattivo, basato su una check-list di conformità, là dove il Regolamento europeo si ispira ad una logica proattiva, il cui baluardo è rappresentato dal principio della *privacy by design*. L'UE, caratterizzata da sistemi sanitari tendenzialmente pubblici, pone l'accento sull'equità nell'accesso alla sanità digitale; gli USA, maggiormente orientati al mercato, si concentrano sugli standard di rimborso e sulla necessità di licenze professionali interstatali, mostrando minore attenzione per il pericolo del *digital divide* nella fruizione di servizi digitali avanzati. Ancora, l'HIPAA ha come principale obiettivo la fluidità dei dati all'interno del sistema sanitario onde ridurne i costi e migliorarne l'efficienza; il GDPR si propone, invece, di garantire al paziente un controllo costante sulla propria "om-

[40] Il sei gennaio 2025, a causa dell'impennata di attacchi ransomware nel settore sanitario, il Dipartimento della Salute statunitense (HHS) ha pubblicato una proposta di riforma che elimina la distinzione tra misure di sicurezza "obbligatorie" e "indirizzabili" - queste ultime implementabili solo se ritenute ragionevoli -, per standardizzare la protezione dei dati (ePHI) in tutte le strutture, indipendentemente dalla dimensione.

bra digitale". I dati dei pazienti americani sono, per di più, facile preda di brokers una volta de-identificati, una pratica che il GDPR cerca di prevenire con definizioni molto più rigide di anonimato.

La legge americana presenta innegabili profili di criticità sul fronte dell'anonimizzazione dei dati – permane ad esempio la possibilità attraverso l'incrocio di database diversi (*data-triangulation*) di risalire all'identità del paziente –, e della confidenzialità: nel caso di utilizzo di app per il monitoraggio della salute, i dati sono protetti dall'HIPAA solo dopo essere stati condivisi con il medico, rimanendo soggetti, prima di questo momento, solo ai termini di servizio e alla *privacy policy* dell'app stessa. Ciò equivale a dire che la confidenzialità dei dati sanitari negli USA è un obbligo soltanto per chi fa parte del sistema sanitario tradizionale, ma non per gli attori che non rientrano nelle categorie dei *covered entities* (le App consumer).

Perplessità circondano, poi, l'impatto dell'IA sulle previsioni normative: la necessità di enormi quantità di informazioni per l'addestramento delle macchine mal si concilia con il rigido quadro dell'HIPAA in materia di autorizzazioni, le quali, da una parte, fungono da freno all'innovazione, e, dall'altra, appaiono come strumenti di difesa troppo deboli avverso algoritmi capaci di dedurre dati sanitari da comportamenti che nulla hanno a che fare con la salute dell'individuo, come gli acquisti online.

A fronte di questi rilievi, la stessa dottrina[41] d'oltre oceano si è vista costretta a prendere atto delle profonde falle strutturali del modello domestico, giudicate responsabili dell'edificazione di un sistema di riservatezza piuttosto che di vera e propria *privacy*. Non a caso, come si è osservato, il dibattito scientifico si è arricchito, nell'ultimo biennio, di significative modifiche che hanno interessato l'*Act* per ciò che concerne la cybersicurezza ed i rapporti tra *privacy*, salute riproduttiva e dipendenze da sostanze. La citata *Reproductive Health Care Privacy Rule*, ancorché depotenziata da una prassi giurisprudenziale di segno

[41] In termini critici rispetto al modello delineato dall'HIPAA si esprime C.J. Mckinstry, *The HIPAA Privacy Rule: Flawed Privacy Exposed When Compared with the European Union's General Data Protection Regulation*, in *Journ. of Healthcare Finance*, vol. 45, n. 1, Summer 2018, p. 1 ss.

affatto riformista, ha stimolato appassionate riflessioni sul tema, sensibilissimo, dell'aborto, riaprendo la vexata quaestio del diritto all'autodeterminazione[42] nelle scelte attinenti alla riproduzione e della opzione tra *federa*l e *state law* nella disciplina di questa incandescente materia.

Le fragilità del modello HIPAA tradiscono, a ben vedere, una precisa scelta di *policy* (oltre che una più blanda accezione della *privacy*). Diversamente da quanto è dato registrare in Europa, l'approccio regolatorio alla sanità digitale si muove su un unico registro, la tutela delle libertà economiche e del mercato, ed in assenza di un quadro epistemologico di riferimento. Se l'*European Health Data Space* (EHDS), adottato recentemente con Regolamento EU 2025/327 per facilitare la circolazione dei dati tra i paesi membri per fini di ricerca e cura, testimonia, in linea di ideale continuità con il GDPR[43], la costante attenzione del legislatore del vecchio continente per la dialettica pubblico/privato e per le plurime dimensioni implicate nell'uso delle informazioni sanitarie - l'etica, il diritto, la sicurezza informatica, il consenso individuale, la tutela della salute, l'interesse della collettività -, l'*Act* misconosce la distinzione tra uso primario dei dati, trattati per finalità di assistenza sanitaria, ed uso secondario, rivolto cioè al loro successivo da parte di soggetti terzi, che è poi l'anima dell'EHDS[44]. La dichiarata ambizione

[42] In argomento cfr. A. Di Martino, *Donne, aborto e Costituzione negli Stati Uniti d'America: sviluppi dell'ultimo triennio*, in *Nomos*, 2022, n. 2, p. 5 ss., e, in termini più generali, S. Cacace, *Autodeterminazione, paternalismo e responsabilità: l'uso dei dati sanitari nella relazione di cura e di fiducia tra medico e paziente*, in *Responsabilità medica*, 2025, n. 3, p. 6 ss.

[43] L'istituzione dello Spazio Europeo dei Dati Sanitari (EHDS) si propone un duplice obiettivo: facilitare le cure e creare un'infrastruttura comune per facilitare lo scambio transfrontaliero e l'uso secondario dei dati sanitari per finalità di ricerca. L'EHDS si propone di bilanciare la libera circolazione con la tutela della privacy, imponendo standard rigorosi di anonimizzazione/pseudonimizzazione e di sicurezza informatici.

[44] Uno dei pilastri del regolamento è la distinzione tra uso primario - l'uso dei dati per la cura del paziente e il loro riutilizzo per altri scopi che permette ai cittadini di accedere gratuitamente ai propri dati sanitari elettronici (cartelle cliniche, ricette, esami) e di condividerli con professionisti sanitari in tutta l'UE – ed uso secondario, che disciplina l'accesso ai dati da parte di ricercatori, istituzioni e aziende per finalità di ricerca, innovazione e salute pubblica. Per una compita analisi dell'EHDS cfr. S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, in *Le nuove leggi civ. comm*., 2025, n. 3, p. 563 ss. G. Di Stefano, *Lo spazio europeo dei dati Sanitari: verso un nuovo paradigma di circolazione e governance del dato tra GDPR e Data Act*, in *Diritto di internet*, 2025, n. 1, p. 45 ss.

del recente Regolamento sullo Spazio Europeo dei Dati Sanitari, è, invero, «creare un'architettura giuridica di condivisione dei dati sanitari, resa operativa da due infrastrutture tecnologiche distinte, MyHealth@ eu e HealthData@ eu, operanti su due livelli»[45], l'individuo e la collettività. L'HIPAA difetta, per di più, di una cornice etica, filosofica e di politiche pubbliche nella quale collocare il fenomeno digitale, a vantaggio di un approccio regolatorio che privilegia l'utilizzo squisitamente commerciale delle informazioni sanitarie[46].

Le pur appariscenti differenze esistenti tra i modelli oggetto di indagine non devono, tuttavia, indurre a sottacere la tendenza dei sistemi giuridici, imputabile soprattutto alla spinta di organizzazioni globali e regionali come l'UE, a convergere su problematiche comuni. L'*e-Health* è una materia che, nell'evolvere assai rapidamente, amplifica le istanze di tutela connaturate all'utilizzo di nuove e sempre più sofisticate tecnologie, sollevando, ovunque, i medesimi interrogativi. Nella sanità digitale, e nella telemedicina in particolare, riservatezza, protezione dei dati e sicurezza reclamano protezione da parte dell'ordinamento giuridico[47], ponendo delicati problemi di bilanciamento tra confliggenti interessi.

L'uso di sistemi di intelligenza artificiale e di dispositivi medici digitali, come quelli in uso nella diagnostica da remoto, postula, in primo luogo, la scelta di un modello di allocazione dei rischi capace di coniugare regole consolidate ed innovazione tecnologica. Sotto questo profilo, non sfugge che la dicotomia tra ordinamenti giuridici *fault based* e *no-fault based* appaia sempre più sfumata. Gli ultimi trenta anni di dibattito intorno alla responsabilità medica hanno dimostrato che i si-

[45] Testualmente, M. Catanzariti, *Lo spazio europeo dei dati sanitari: una riflessione interdisciplinare su diritto, etica e scelte pubbliche*, in notizie di *Notizie di Politeia*, XLI, 158, 2025, p. 5.

[46] Lo rileva R. Sala, *Lo spazio europeo dei dati sanitari: una questione di etica pubblica*, in *Notizie di Politeia*, vol. XLI, n. 158, 2025, pp. 7-17.

[47] «[…] la riservatezza, la protezione dei dati e la sicurezza potrebbero essere viste sia come questioni relative alle tecnologie di e-health sia come diritti o obblighi stabiliti dalla legge per ridurre al minimo i rischi per i diritti e le libertà degli individui» (testualmente P. Guarda, in G. Bincoletto - P. Guarda, *Diritto comparato della privacy e della protezione dei dati personali*, cit., p. 298.

stemi giuridici tradizionalmente fondati sulla colpa - Italia, Germania, Francia, e, nel *common law*, il Regno Unito - si sono avvalsi nel tempo, specie sul piano probatorio[48], di strumenti di oggettivizzazione o di semi oggettivizzazione della responsabilità per facilitare il risarcimento della vittima, riducendo notevolmente il gap rispetto a ordinamenti – come quello nordamericano – orientati verso una responsabilità "senza colpa". Tendenza che l'ITC ha amplificato, attraendo la *medical malpractice* nell'alveo della responsabilità da prodotto difettoso[49].

Parimenti condivisa è la preoccupazione di individuare un ragionevole equilibrio tra le nuove frontiere della scienza medica, l'interesse pubblico ed i diritti fondamentali dell'individuo. Il miglioramento dell'efficienza e della qualità dell'assistenza sanitaria che indubbiamente va ascritto all'*e-health* nelle sue diverse declinazioni deve fare i conti con la natura ultra-sensibile del dato sanitario ("categoria particolare di dati personali" nel linguaggio del GDPR), la cui digitalizzazione ne aumenta esponenzialmente il valore, ma, nel contempo, i pericoli nell'utilizzo. Sotto questo profilo, assume particolare significato la qualificazione operata dal legislatore europeo con l'*AI Act* dei sistemi di intelligenza artificiale destinati a scopi medici come "ad alto rischio". Tanto comporta requisiti rigorosi in termini di gestione degli eventi avversi, qualità dei dati, tracciabilità, trasparenza e sorveglianza umana, definendo standard di sicurezza che, se rispettati, forniscono una adeguata protezione sia il paziente, sia all'operatore sanitario. Il Regolamento europeo sull'intelligenza artificiale configura una "accountability" in capo agli sviluppatori ed agli utilizzatori di sistemi di IA, la quale, non è superfluo precisarlo, si aggiunge, ma non si sostituisce, alle norme vigenti

[48] Sul tema sia consentito il rinvio a L. Saporito, *Responsabilità medica, tecniche probatorie, intelligenza artificiale*, a cura di Aa.Vv., *Il valore del dissenso. Riflessioni con Vincenzo Zeno-Zencovich*, Roma Tre Press, 2025, p. 1311 ss.

[49] In argomento, tra i numerosi contributi dedicati a questo complesso tema, cfr. C. Scognamiglio, *Responsabilità civile ed intelligenza artificiale: quali soluzioni per quali problemi?*, in *Resp. civ. prev.*, 2023, n. 4, p. 1082 s.; L. Buonanno, *La responsabilità civile nell'era delle nuove tecnologie: l'influenza della blockchain*, in *Resp. civ. prev.*, fasc. 5, 2020, p. 1618; M. Infantino, *La responsabilità per danni algoritmici: prospettive europeo-continentali*, in *Resp. civ. prev.*, 2019, n. 5, p. 1762 ss.

nei paesi europei in materia di responsabilità sanitaria (in Italia, alle previsioni della legge Gelli-Bianco).

Accanto alla scelta degli strumenti tecnici regolatori del fenomeno, l'e-health solleva questioni, anch'esse trasversali alle diverse esperienze giuridiche, di ordine etico. La digitalizzazione reca indubbiamente con sé il pericolo della «smaterializzazione dell'esperienza cognitiva ed emotiva», della «virtualizzazione dei rapporti umani»[50]. Nella cibermedicina, in particolare, il passaggio dalla "presenza" alla "connessione" produce una metamorfosi della relazione medico-paziente, filtrata da strumenti che integrano e, talvolta, sostituiscono segmenti di una interazione affidata, fino ad un tempo recente, esclusivamente alla comunicazione verbale, al tono della voce, allo sguardo e alla gestualità. Il corpo del paziente diviene un insieme di dati, pixel e parametri biometrici che il medico gestisce attraverso una comunicazione burocratica e fredda. V'è il rischio, si osserva, che la tecnologia prenda il sopravvento sul giudizio critico, che il medico si affidi ciecamente agli output di una macchina, che il consenso diventi una mera spunta su una casella[51]. Bisogna tuttavia diffidare da talune, paternalistiche narrazioni intorno al cd. "dis-umanesimo digitale". Alla retorica sulla teocrazia degli algoritmi[52] può replicarsi che, malgrado l'impiego della tecnologia nella scienza medica, la regia resta quella umana. La digitalizzazione funge da *augmentative tool*, potenziando le abilità del medico, senza mai sostituirsi ad esso. L'e-health non può essere insofferente a norme[53], giuridiche e morali, a meno che il diritto abdichi alla dimensione regolatoria che gli è propria, trincerandosi dietro il principio di neutralità tecnologica.

[50] Testualmente A. Punzi, *L'umanesimo digitale: verso un nuovo principio di responsabilità*, in *Democrazia e diritti sociali*, 2023, n. 1, p. 24

[51] Per questi rilievi cfr. U. Izzo, *Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina*, in *Danno e resp*., 2000, p. 807 ss.

[52] In argomento cfr. B. Romano, *Algoritmi al potere. Calcolo giudizio pensiero*, Giappichelli, 2018; A. Rouvroy - B. Stiegler, *Il regime di verità digitale. Dalla governamentalità algoritmica a un nuovo Stato di diritto*, in *La Deleuziana*, 2016, n. 3.

[53] Sul tema v. N. Irti - E. Severino, *Dialogo su diritto e tecnica*, Roma-Bari, 2001.

EMERGING TECHNOLOGIES AND THE EVOLUTION OF PRIVATE LAW

BLOCKCHAIN E SMART CONTRACT: PROFILI DI VULNERABILITÀ NELLE DECENTRALIZED AUTONOMOUS ORGANIZATION

Antonio Tipaldi

Sommario: 1. La tecnologia *blockchain* al servizio delle *Decentralized Autonomous Organization* (DAO) funzionamento e sicurezza. – 2. Fisionomie di *cibersecurity* negli *smart contract* e nelle DAO. – 3. Il "*Data Act*" quale possibile volano per le DAO.

1. La *blockchain* appartiene alla categoria dei *database* ma se ne differenzia perché è un registro decentralizzato e strutturato come una catena di blocchi contenenti le transazioni delle informazioni, la cui validazione è affidata a un meccanismo di consenso distribuito su tutti i nodi partecipanti della rete, in pratica su tutti i nodi che sono autorizzati a partecipare al processo di validazione delle transazioni da includere nel registro.

Tale tecnologia, rappresenta, inoltre, una soluzione per creare *asset* digitali unici, ovvero mantenere l'unicità di documenti ed escludere la loro duplicazione.

Esistono diverse declinazioni, interpretazioni e definizioni della *blockchain*, quella più conosciuta è sicuramente la *blockchain Bitcoin*, la cui nascita è attribuita a Satoshi Nakamoto che nel suo libro pone una definizione tecnica e fortemente politica di moneta digitale ovvero «*We define digital coin as a chain of digital signatures*»[1], considera essa come un paradigma tecnologico associato ad un concetto di moneta virtuale e i c.d. *bit coin* quali ulteriori paradigmi tecnologici composti da stringhe uniche di numeri e lettere che costituiscono una moneta virtuale, non emessa da una banca centrale o da un'autorità pubblica,

[1] S. Nakatomo *Bitcoin: A peer-to-peer Electronic Cash System*, in *https://bitcoin.org/bitcoin.pdf.*

utilizzata come strumento di pagamento ma anche come strumento di finanziamento per le imprese.

A riguardo, si parla di *Initial Coin Offerings* (ICO) per indicare una raccolta di risorse sotto forma di cryptovalute, per la realizzazione di progetti tecnologici basati su *blockchain*.

In generale, la tecnologia *blockchain* ha un grande valore anche in settori completamene diversi, essendo la base di tutti i sistemi *AI* per le funzioni e utilità che vengono spiegato di seguito; si tratta di un fenomeno assolutamente recente che ha vissuto una serie importante di accelerazioni e che ha creato molte aspettative; le componenti essenziali della *blockchain* sono: *Ledger*, Nodo, Blocco, *Hash, Miner, Token*[2].

Il *Ledger*, c.d. "Libro Mastro"[3], base fondamentale della contabilità, nei propri archivi contiene una serie di dati che permettono di definire delle regole di analisi, di controllo, di verifica ad esempio delle transazioni commerciali di una azienda o degli atti di una Pubblica Amministrazione; grazie alla digitalizzazione, anche tale fondamentale documento contabile è diventato virtuale.

Il fenomeno della *Digital Transormation* ha aperto l'era dell'economia immateriale e ha le sue basi proprio sulla capacità di rendere disponibile un bene o servizio ad esempio un *software*, un brano musicale o un *ebook,* tanto ad un cliente quanto a milioni di clienti esattamente nella stessa identica forma a costi marginali infinitamente più bassi rispetto alle logiche del mondo materiale[4].

Il *Digital Ledg*er si basa su un insieme di blocchi incatenati tramite una funzione di criptografia, di sviluppo di algoritmi di controllo e di

[2] G. Chiap - J. Ranalli - R. Bianchi, *Blockchain. Tecnologia e applicazioni per il business*, Hoepli, 2019, pp. 15-31, 53-57, 110.

[3] Insieme al Libro Giornale, è uno dei documenti fondamentali per la tenuta della contabilità generale; questi due registri sono tra loro strettamente collegati, in quanto, tutti i fatti esterni di gestione vengono riportati: nel libro giornale in modo cronologico, cioè in ordine di data; nel libro mastro in modo sistematico, cioè in base all'oggetto al quale di riferiscono; Cfr. S. Giordano, *Manuale delle scritture contabili 2023*, Maggioli Editore, 2023, pp. 1-18.

[4] M. Ciancia - M. Ronchi, *Digital transformation. Metodi e strumenti per guidare l'evoluzione digitale delleimprese attraverso design, marketing e comunicazione*, Franco Angeli, 2019, paragrafi 2.1 e 2.2.

verifica dei dati; solo capendo la *Distributed Ledger Technology*[5], è possibile comprendere come questo sistema possa essere utilmente usato per risolvere i problemi di *governance*.

Le tante utilità correlate possono essere sintetizzate nei concetti di libero accesso, trasparenza, sicurezza, immutabilità e convenienza.

La *blockchain* non è altro che un *Distributed Ledger*, un registro distribuito, in cui vengono "annotate" con la massima trasparenza e in modo immutabile tutte le transazioni effettuate in modo ordinato e sequenziale.

Tale registro è pubblico in quanto viene condiviso su più computer nello stesso momento, tutti perfettamente sincronizzati su tutti gli stessi documenti; l'operazione, una volta ottenuto il consenso, aggiunge un nuovo blocco alla catena ed aggiorna il Libro Mastro detenuto da tutti i partecipanti alla *blockchain*, con l'ultima versione di ogni singola operazione di ciascun partecipante.

Ovviamente, ogni operazione rimane poi in modo indelebile e immutabile su ogni singolo nodo[6].

Le transazioni, i passaggi e gli scambi non sono più gestiti sotto il controllo rigoroso di una autorità centrale, che verifichi, controlli e autorizzi le varie richieste, ma sono invece creati e caricati da ciascun nodo in modo indipendente, ma sotto il controllo consensuale degli altri nodi.

Non vi è più una struttura centralizzata, ma un sistema chiamato *Peer to Peer* non c'è più un unico Libro Mastro, ma più libri mastri di cui tutti gli utenti hanno una copia potendolo controllare, visionare, e, a fronte di regole che vanno a comporre il protocollo di funzionamento della *blockchain,* possono modificarlo.

È chiaro, dunque, che si tratta di un sistema nella pratica più conveniente per portare a termine delle transazioni commerciali, ci sono meno interlocutori di terze parti, necessari in tutte le transazioni

[5] A. Sunyaev, *Distributed Ledger Technology*, in *Internet Computing*, Springer, 2020, pp. 265-299.

[6] R. Garavaglia, *Tutto su Blockchain. Capire la tecnologia e le nuove opportunità*, Hoepli, 2018, p. 11 ss.

convenzionali che avvengono tra due o più parti (banche e altri enti simili).

Il "Nodo" è costituito fisicamente da un dispositivo col compito di validare le transazioni delle informazioni che avvengono nella rete; nella *blockchain,* ogni operazione effettuata viene confermata da tutti i singoli nodi, attraverso software di crittografia, che verificano il corretto trasferimento di un pacchetto di informazioni.

Il "Blocco" è l'involucro di una serie di transazioni, costituite dai dati che rappresentano i valori oggetto di "scambio" e che necessitano di essere verificati, approvati e poi archiviati; contiene informazioni relative all'indirizzo pubblico del ricevente, le caratteristiche della transazione e la firma crittografica che garantisce sicurezza e autenticità della transazione.

Essa viene verificata da parte dei partecipanti alla *blockchain*, ai fini dell'approvazione; se le informazioni sono considerate corrette, la transazione viene autorizzata, validata ed effettuata e quindi entra a far parte di un nuovo blocco che si aggiunge alla catena degli altri blocchi, accessibile a tutti i partecipanti ed inserita nell'archivio di tutti i partecipanti, diventando il riferimento permanente, immutabile e immodificabile di quella specifica transazione[7].

Dando a tutti i partecipanti una parte di controllo, più o meno ampia, dell'intera catena, la *blockchain* diventa un sistema più sicuro e affidabile; invero, se solo uno dei nodi della catena subisce un attacco e si danneggia, tutti gli altri nodi del database distribuito continueranno comunque a essere attivi e operativi, saldando la catena e non perdendo informazioni importanti.

Una volta inserite nella *blockchain*, le informazioni sono irrevocabili e definitive, senza alcuna possibilità di essere modificate o annullate, così più facilmente tracciabili; se esistesse un unico Libro Mastro, basterebbe modificarlo o danneggiarlo, ma nella *blockchain* non esiste un'autorità centrale, quindi sarebbe necessario modificare o danneggiare simultaneamente tutte le copie del libro mastro possedute da tutti i partecipanti.

[7] J. De Tullio, *La matematica dei minatori della blockchain*, in *MATEpristem*, 2018, pp. 1-5.

L'immutabilità dell'operazione soddisfa poi l'esigenza di sicurezza: all'interno di ogni nuovo blocco viene indicata una specifica sequenza di caratteri, definita *Timestamp* (marca temporale), che identifica in modo univoco, indelebile e immutabile una data e/o un orario per fissare e accertare l'effettivo avvenimento di un certo evento, permettendone la comparazione con altre date definendo un ordine temporale finale; la "Marca Temporale", associando una data e un'ora certe a un documento informatico, impedisce che l'operazione venga alterata o annullata, consentendo di definire una validazione temporale che può essere opponibile a terzi.

Dal punto divista delle "regole di gestione", ciascun blocco si "aggiunge" alla catena sulla base di un processo basato sul consenso distribuito su tutti i nodi della rete, ovvero con la partecipazione di tutti i nodi che vengono chiamati a contribuire alla validazione delle transazioni presenti in ciascun blocco e alla loro "inclusione" nel registro; in una *blockchain*, ancor di più se di natura pubblica i dati vengono mantenuti su ogni nodo della rete (pubblicamente accessibile a chiunque) indipendentemente dallo scopo originale per cui quei dati sono stati immessi ed elaborati nella *blockchain*[8].

L'*Hash* è l'algoritmo che consente di saldare una stringa di testo e/o numerica di lunghezza variabile in una stringa unica ed univoca di lunghezza determinata fissa, chiamata "Valore di *hash*", consentendo di identificare in modo univoco e sicuro ciascun blocco, ed ogni modificaprodurrà una diversa stringa in uscita; in tal modo vengono registrate tutte le informazioni relative al blocco permettendo di creare la catena e di legare un blocco all'altro[9].

La peculiarità di questo algoritmo è la sua funzione crittografica, in virtù della quale, dato un valore di *hash*, sarà molto difficile risalire al messaggio che l'ha generato; risulterà impossibile riprodurre un messaggio con lo stesso valore di *hash* e sarà altrettanto impossibile gene-

[8] Cfr. R. Guariglia, *Conoscere la blockchain. For Dummies*, Hoepli, 2021; R. Garavaglia, *Tutto su Blockchain. Capire la tecnologia e le nuove opportunità*, Hoepli, 2018; L. Foti, *Capire Blockchain*, Amazon Distribution S. D., 2017.

[9] S. Lovati, *Algoritmi di hash e loro utilizzo nelle criptovalute*, in *https://it.emcelettronica.com/algoritmi-di-hash-e-loro-utilizzo-nelle-criptovalute*, 2019.

rare un messaggio dal suo valore *hash* se non provando tutti i messaggi possibili[10].

Tali caratteristiche permettono alle funzioni crittografiche di *hash* di trovare ampio utilizzo negli ambiti della sicurezza informatica, quali forme di autenticazione.

Il *Miner*[11] è il nodo che svolge l'attività di *mining*, ovvero la ricerca della soluzione all'algoritmo di *hash* al fine di validare e crittografare il nuovo blocco che si è aggiunto alla catena, cosa che richiede un cospicuo impegno anche in termini di potenza e di capacità elaborativa.

L'algoritmo di *hash* è concepito per mettere in competizione tutti i nodi, ciascuno dei quali tenterà di risolvere con la propria potenza di calcolo; il primo che riesce a risolverlo avrà il diritto di validare il blocco con la presentazione della "*Proof of Work*", ovvero la prova della soluzione, usata come modo per costruire un rapporto di "fiducia" basato sulla concreta collaborazione alla soluzione delle prove che devono essere validate[12].

Nella maggior parte dei casi, il primo *miner* che crea un blocco valido e lo aggiunge alla catena viene ricompensato con la somma delle commissioni per le sue transazioni, attraverso degli *asset* digitali.

Nel caso in cui il processo di verifica dovesse rilevare un errore, un'anomalia, una discrepanza, il blocco viene rifiutato e tutti hanno visibilità del fatto che la transazione non è stata autorizzata.

Se invece tutte le transazioni sono validate, il blocco viene creato e aggiunto ed entrerà a far parte della *blockchain* a tutti gli effetti come un *record* pubblico permanente e immutabile; nessun partecipante alla *blockchain* potrà cambiarlo o rimuoverlo.

Torna utile precisare che la *blockchain* si caratterizza per una logica distribuita e di *governance* costruita attorno a un nuovo concetto di

[10] I. Ahmad, *40 algoritmi che ogni programmatore deve conoscere. Per migliorare nel problem solving e scrivere codice più efficace*, Apogeo, 2022, pp. 252-256.

[11] Il *miner* è un nodo speciale del *network* che mette a disposizione i suoi computer per il processo di *mining*; i *miner* sono incentivati a fare questo lavoro perché a ogni blocco creato guadagnano una ricompensa per ogni blocco estratto e in più guadagnano anche le commissioni presenti all'interno delle transazioni (chiamate *fee*). Cfr. P.N. Tan - M. Steinbach, *Introduction to Data Mining*, (USA), Financial Times Press, 2019, p. 71 ss.

[12] A. Rubino, *Proof of work: cos'è e le differenze con il proof of stake*, in *NetWork 360*, 2020.

fiducia tra tutti i soggetti, nessuno ha la possibilità di prevalere e il processo decisionale passa rigorosamente attraverso un processo di costruzione del consenso. Tuttavia, esistono algoritmi di gestione della raccolta del consenso e delle approvazioni di operazioni, tale sistema non è solo il più conveniente, ma anche quello più trasparente, in quanto le transazioni effettuate sono visibili a tutti i partecipanti. L'identità e i dati sensibili di un utente sono protetti da un codice che rappresenta la chiave pubblica per aderire alla rete distribuita; questi i modelli di gestione del consenso determinano la differenza tra *blockchain* di tipo "pubblico" o anche *Permissionless Ledger* e di tipo "privato" o anche indicata come *Permissioned Ledger*[13].

La prima è aperta, nel senso che non hanno una "proprietà" o un attore di riferimento, in quanto concepite per non essere controllate, così ogni partecipante può contribuire all'aggiornamento dei dati e disporre di tutte le copie immutabili di tutte le operazioni approvate grazie al consenso. Allo stesso tempo, nessuno può impedire che una transazione possa avvenire e che possa essere aggiunta al *ledger* una volta che ha conquistato il consenso necessario tra tutti i nodi alla; infatti, l'attività di *mining* può essere svolta da qualsiasi partecipante e il *miner* viene incentivato con forme di remunerazione definite da ciascuna *blockchain.*

Questo tipo di *ledger* viene utilizzato come database globale per tutti quei documenti che hanno la necessità di essere assolutamente immutabili nel tempo a meno di aggiornamenti che richiedono la massima sicurezza in termini di consenso (ad es. i contratti di proprietà); in tal caso, la *governance* è definita dalla struttura della *blockchain.*

La seconda, ovvero la *Permissioned Ledger*, utilizzata da istituzioni, grandi imprese, banche e società di servizi, non è aperta ma bensì controllata, in quanto di "proprietà" di un limitato numero di attori definiti *Trusted*; ogni partecipante opera in modo indipendente, ma viene controllato dai *Trusted.*

Questa tipologia è caratterizzata da una *governance* particolare, con speciali regole, condivise da tutti gli attori, per l'accesso e la visibilità dei dati, e di comportamento, che rende la *blockchain* più performante

[13] I. Serrai, *Blockchain: Permissionless vs Permissioned*, 27 giugno 2022, in *https://www.ictsecuritymagazine.com/articoli/blockchain-permissionless-vs-permissioned/#.*

e veloce delle *Permissionless ledger*; infatti, in questo caso, il ruolo del *miner* è svolto, in funzione della *governance*, dall'autorità che attiva la *blockchain* stessa.

In tal modo, la *governance* diventa parte integrante del processo progettuale e rappresenta la base sulla quale vengono poi attuate le attività di produzione, garantendo prima di tutto l'assoluta sicurezza della *blockchain* e naturalmente il raggiungimento degli obiettivi di business delle imprese e delle organizzazioni che la utilizzano[14].

Il *Token*, anche noto come *trusted device*, è un insieme di informazioni digitali all'interno di una *blockchain* che conferisce un diritto a un determinato soggetto; la "tokenizzazione" è la conversione dei diritti di un bene in un *token* digitale registrato su una *blockchain*[15].

In verità al termine *token* si possono attribuire due significati distinti e altrettante peculiarità, a seconda del contesto in cui questo termine viene usato, ovviamente il settore a cui si fa riferimento più spesso per attribuire un primo significato di *token* è quello delle criptovalute, infatti partendo dal presupposto che una criptovaluta è una "moneta elettronica" basata su *blockchain* o su altro registro distribuito, possiamo sicuramente dire che ciascuna di queste criptovalute come ad esempio Bitcoin, Ethereum ecc., ha un suo proprio registro delle transazioni sul quale vengono memorizzati gli scambi[16].

I *token*, che in questo caso potremmo definire "gettoni" sono di fatto frazioni di una criptovaluta emessa, che vengono scambiati tra gli utenti mediante scambi che vengono memorizzati sul suddetto registro.

Esiste poi un'altra tipologia di "gettone" chiamato anch'esso *token,* che a differenza di quelli di cui sopra, non ha un proprio registro, ma utilizza il registro di un'altra *coin*; ad esempio, mediante *gli smart contract* di *Ethereum*[17]*,* chiunque può emettere i suoi propri *token*, per

[14] Aa.Vv., *Blockchain & Distributed Ledger: aspetti di governance, security e compliance*, Clusit (AssociazioneItaliana per la sicurezza informatica), pp. 8/14, in *https://clusit.it/wp-content/uploads/docs/BC-e-DLT-Governance- Security-Compliance-v1.pdf.*

[15] Aa.Vv., o.u.c., pp. 21/24.

[16] P. Mascherin, *Nft, token e crypto, cosa resterà di questo 2022*, *in https://www.we-wealth.com/news/pleasure-assets/art-tech/nft-token-e-crypto-cosa-restera-di-questo-2022.*

[17] G. Albè - F. Bottini, *Ethereum, il luogo virtuale dove nascono smart contract e Nft*, in *Network Digita*l 360, sezione *Blockchain4.Innovation*, 2021.

esempio con una *Initial Coin Offer* (ICO) e registrare le transazioni afferenti quel *token* sulla *blockchain* di *Ethereum* invece che necessariamente costruirne una propria.

Il *token* ha quindi le stesse caratteristiche della criptomoneta ovvero sicurezza e trasferibilità non censurabili ma non è "nativo" e soprattutto "interno" alla *blockchain* sulla quale vengono memorizzate le transazioni che lo riguardano ma rappresenta il gemello digitale di un bene reale, un diritto "reale", ma che esiste di fuori del sistema *blockchain.*

Sperando di aver chiarito questa prima differenza e focalizzando l'attenzione sul termine *token* inteso quale "gettone" creato utilizzando una *blockchain* di una *coin* esistente, possiamo sicuramente affermare che un *token* è un insieme di informazioni digitali all'interno di una *blockchain* che conferiscono un diritto a un determinato soggetto.

La c.d. "tokenizzazione" rappresenta la procedura di conversione dei diritti di un bene in un *token* digitale registrato su una *blockchain*, dove il bene reale e il *token* sono collegati da uno *smart contract*[18].

"Tokenizzare", quindi, significa generare un *token* nel mondo virtuale e collegarlo a un bene esistente nel mondo reale mediante l'utilizzo degli *smart contract*[19].

In conclusione la *blockchain,* consente la soluzione alle problematiche e rischi riferibili all'esigenza di trasparenza: nella *blockchain* ogni operazione può essere rintracciata in ogni momento in base alla chiave privata, ma si tratta di un'individuazione esclusivamente sul piano tecnico-temporale, nel senso che non identifica in maniera inequivocabile il soggetto che ha compiuto l'operazione, o gli scopi che hanno spinto l'operatore a effettuare l'operazione, ostacolando l'intercettazione delle comunicazione, il sequestro e la confisca delle cryptovalute.

Il problema è più grave di quanto sembri, basti pensare che nel caso delle cryptovalute in cui per l'utilizzazione dei *wallet* (portafogli

[18] L. Rey Rodriguez, *La tokenizzazione degli asset: che cos'è e cosa comporta per i mercati*, 8 marzo 2022, in *https://fundspeople.com/it/glossario/la-tokenizzazione-degli-asset-che-cose-e-cosa-comporta-per-i-mercati/.*

[19] C. Robustella - E. Papadimitriu, *Spunti ricostruttivi in tema di smart contract, tra innovazione tecnologica e regola giuridica*, in *Persona e Amministrazione*, X, 1/2022, pp. 963-996; A. Vercellotti, *SmartContract. Che valore legale hanno*, del 14/06/2022, in *https://legalfordigital.it/nft/smart-contracts-blockchain/.*

elettronici) ovvero dei *digital ledger* portatili sarà sufficiente possedere e utilizzare un nome "ID" e una *password* caratterizzate da lunghissime sequenze crittografiche; non ci sono altre tracce che possano ricondurre all'identità fisica e personale dell'operatore, tant'è vero che tali portafogli sono considerati giuridicamente dei titoli al portatore.

La sicurezza della blockchain costituisce uno degli elementi fondamentali per il successo delle applicazioni blockchain nel contesto aziendale, i principali rischi associati all'utilizzo di tale tecnologia riguardano in particolare possibili attacchi informatici come ad esempio il Denial-of-Service in cui viene sfruttato un programma per inondare la rete di transazioni, superando la capacità massima della blockchain e rendendo il sistema non disponibile; questi attacchi sovraccaricano la rete rendendola temporaneamente inadoperabile e compromettendone la fiducia[20].

Ulteriore punto debole è rappresentato dalla sicurezza degli *endpoint* ovvero i punti di accesso alla rete blockchain come ad esempio desktop e laptop ma anche smartphone, tablet e POS.

Tali strumenti sono soggetti spesso a fenomeni di *"phishing"* in cui terze parti utilizzano e-mail fraudolente o altre comunicazioni digitali per indurre ad esempio i dipendenti di un'azienda a rivelare informazioni sensibili. A riguardo, esistono soluzioni avanzate di sicurezza degli *endpoint* che incorporano gateway e-mail per identificare e mettere in quarantena le e-mail dannose, riducendo così il rischio di cadere in tattiche di *phishing*.

2. L'evoluzione della tecnologia *blockchain* ha rivoluzionato le categorie classiche del diritto civile e commerciale, introducendo nuove forme giuridiche e nuovi strumenti meritevoli di tutela da parte dell'ordinamento[21].

[20] M. Valeri, *Attacchi alla blockchain: cause, conseguenze e contromisure*, in *Nextwork360*, 2019.

[21] Negli ultimi anni la tecnologia blockchain sta spingendo il diritto civile verso nuove frontiere, introducendo sfide e opportunità nel contrattualistica digitale, nella tutela della proprietà, nella gestione dei dati e nell' identità digitale, richiedendo l'adattamento di principi tradizionali come la buona fede e la lealtà ai nuovi strumenti (*smart contracts*, NFT, DAO), ma sollevando questioni cruciali su privacy, scalabilità e l'equilibrio tra innovazione tecnologica e diritti fondamentali, necessitando di un quadro normativo flessibile e moderno. A riguardo si veda M. Marletta, *Blockchain e buona fede: riuscirà la tecnologia a sostituire la fiducia?*, in *Riv. it. inf. dir.*, 1/2025, pp. 616-626.

Smart contract e *Decentralized Autonomous Organization* (da qui in avanti DAO) non rappresentano soltanto un'innovazione tecnologica bensì una rivoluzione organizzativa e sociale che ridefinisce la *governance* e l'intermediazione, creando modelli decentralizzati per la gestione di asset, votazioni e processi decisionali, basati su regole codificate e automatiche, eliminando intermediari e offrendo trasparenza[22]. L'analisi del nesso tra *smart contract* e DAO non può prescindere da una corretta inquadratura della fattispecie tecnologica sottostante.

Lo *smart contract*, nell'accezione originariamente proposta da Nick Szabo[23] e successivamente implementata su protocolli blockchain come Ethereum[24], si configura come un protocollo informatico auto-esecutivo.

Sotto il profilo tecnico, esso è un *software* che traduce clausole contrattuali in codice eseguibile, garantendo che, al verificarsi di una condizione prestabilita, la prestazione venga eseguita in modo automatico e irreversibile[25].

[22] A. Manganelli, *Decentralized Autonomous Organization, blockchain e impresa: considerazioni giuridico-economiche*, in *Riv. it. dir. inf.*, 1/2025, pp. 296-297.

[23] La definizione fornita da Nick Szabo è la seguente: «A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs». Szabo aveva anche descritto un sistema decentralizzato di generazione e scambio di moneta digitale denominata "Bit gold", precorritrice dell'odierno e più famoso Bitcoin. Szabo ha altresì auspicato l'utilizzo dello smart contract in ulteriori ambiti, come l'acquisto di un bene a rate, quale l'automobile, ipotizzando un sistema per cui all'inadempimento del compratore consegua un automatico blocco del veicolo attraverso, appunto, l'interazione di un software e un hardware capaci di riconoscere l'avverarsi di una condizione prestabilita (ad esempio, il mancato o ritardato pagamento della rata di periodo), senza che sia necessario, né possibile, un ulteriore intervento umano perché si realizzino le relative conseguenze.

[24] Ethereum è definita come «una tecnologia gestita dalla community che alimenta la criptovaluta ether (ETH) e migliaia di applicazioni decentralizzate». Cfr. *https://ethereum.org/it/*. Si tratta di una piattaforma del c.d. "Web 3.0" per la creazione e pubblicazione peer-to-peer di smart contract, la cui criptovaluta "Eth" è seconda per capitalizzazione solo a "Bitcoin"

[25] Cfr. F. Bassan - M. Rabitti, R*ecenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai "contracts on chain"*, in *Riv. dir. ban.*, Luglio/Settembre 2023, pp. 561-639.

L'ordinamento italiano è stato tra i primi a recepire formalmente tale figura; l'art. 8-ter del d.l. 135/2018, inserito in sede di conversione nella Legge 12/2019, definisce lo *smart contract* come un «programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse». Tale norma attribuisce allo *smart contract* il requisito della forma scritta, previa identificazione informatica delle parti secondo i requisiti fissati dall'Agenzia per l'Italia Digitale (AgID).

A livello sovranazionale, il Regolamento (UE) 2023/2854 (Data Act) ha introdotto una definizione armonizzata, descrivendo il contratto intelligente come un programma informatico utilizzato per l'esecuzione automatica di un accordo, garantendo l'integrità e l'accuratezza dell'ordine cronologico delle registrazioni. L'approccio europeo, pur mantenendo una neutralità tecnologica, pone l'accento sulla robustezza e sulla verificabilità del codice, elementi essenziali per la certezza dei rapporti giuridici nella *data economy*[26].

La *ratio* sottesa agli *smart contract* è spesso riassunta nel brocardo "*code is law*", che postula la sufficienza del codice informatico a regolare integralmente il rapporto tra le parti, escludendo l'intervento di terzi o dell'autorità giudiziaria[27].

Tuttavia, tale visione si scontra con la realtà delle patologie negoziali; in caso di errore di programmazione (bug) o di vizio del consenso, la rigidità della *blockchain* può trasformare un'esecuzione automatica in un'esecuzione indebita.

[26] A riguardo esistono delle differenze sostanziali tra l'approccio normativo europeo e quello nazionale; in particolare l'UE attraverso il regolamento eIDAS 2 punta a creare un quadro giuridico omogeneo e riconosciuto per l'identità digitale e la fiducia, introducendo i "*Qualified Electronic Ledgers*", mentre l'Italia, pur riconoscendo gli Smart Contracts in alcune leggi specifiche ad esempio nel Codice dell'Amministrazione Digitale, si confronta con la necessità di conciliare l'automatismo del codice con i principi del diritto contrattuale tradizionale, soprattutto riguardo validità, nullità e risoluzione, ambito in cui l'Europa offre maggiore chiarezza per la circolazione transfrontaliera. Si veda in tema G. Riccio - A. Toscano, *Gli Smart Contract alla luce di eIDAS 2*, in *Ratio Iuris*, 1/26, p. 230; M. Nicotra, *L'Italia prova a normare gli smart contract, ecco come: pro e contro*, in *Agenda Digitale*, 2019.

[27] V. Sanasi D'Arpe, *Connessioni funzionali tra smart contracts e disciplina generale dei contratti: criticità ermeneutiche e soluzioni applicative*, in *Rivista scientifica trimestrale di diritto amministrativo*, 3/2024, pp. 896-906

La dottrina italiana[28] evidenzia come lo *smart contract* possa assumere una funzione costitutiva del vincolo quando il consenso si manifesta direttamente attraverso l'attivazione del software.

In tale contesto, l'oggetto del contratto deve essere determinato o determinabile (art. 1346 c.c.); la mancanza di tali requisiti nel codice informatico porterebbe alla nullità del negozio, nonostante l'irretrattabilità tecnologica dell'esecuzione.

Le DAO rappresentano una proiezione collettiva degli *smart contract*; esse sono entità che operano senza una direzione centralizzata, basando la propria esistenza e il proprio funzionamento su regole codificate in modo immutabile su una *blockchain*[29]; tali entità spostano il baricentro del controllo dall'individuo, amministratore o dirigente, alla collettività dei partecipanti, i quali esercitano il potere decisionale tramite *governance token*[30].

Il funzionamento di una DAO si fonda su tre pilastri: autonomia, decentralizzazione e trasparenza. Le decisioni vengono prese attraverso vo-

[28] Si veda in tema M. Maugeri, *Smart contracts e disciplina dei contratti*, Il Mulino, 2021, p. 19 ss.; A. Stazi, *Automazione contrattuale e «contratti intelligenti». Gli Smart contract nel diritto comparato,* Giappichelli, 2019; I. Martone, *Gli Smart Contracts. Fenomenologia e funzioni*, ESI, 2022.

[29] A. Manganelli, *Decentralized Autonomous Organization, blockchain e impresa: considerazioni giuridico-economiche*, cit., pp. 292-304.

[30] Un *governance token* è un tipo di criptoasset che conferisce ai detentori diritti di voto sul futuro di un progetto o protocollo blockchain. Possedendo un governance token, gli utenti possono partecipare alle decisioni su proposte importanti all'interno di un progetto. Questo diritto di voto viene spesso applicato all'interno di blockchain o protocolli che utilizzano una DAO (Decentralized Autonomous Organization). I detentori di governance token possono votare su temi come aggiornamenti software, innovazioni (ad esempio l'introduzione di un nuovo meccanismo di staking), modifiche alle commissioni di transazione o la distribuzione di fondi comuni. I governance token sono utilizzati principalmente all'interno di progetti blockchain decentralizzati in cui non esiste un'entità centrale che prende decisioni. Al contrario, il potere è nelle mani della community. Spesso vale la regola secondo cui più governance token possiede una persona, maggiore è il peso del suo voto all'interno del progetto. Ciò significa che i grandi detentori di token hanno più influenza rispetto ai partecipanti più piccoli. Esistono tuttavia anche modelli in cui ogni partecipante ha lo stesso diritto di voto, indipendentemente dal numero di token posseduti. In tema si veda P. Bauer, *Governance-Token*, Mohr Siebeck GmbH & Co. K, 2025; M. Daniele, *Initial Coin Offerings (ICOs), tokenizzazione e crypto governance*, Cedam, 2024.

tazioni *on-chain* registrate pubblicamente; il peso del voto è solitamente proporzionale al numero di *token* detenuti; alcune DAO implementano modelli di voto più complessi, come il voto quadratico, per evitare che una piccola élite formata da grandi detentori di *token*, le c.d. "balene"[31], possa monopolizzare la *governance*. Il principale problema che le DAO pongono agli ordinamenti tradizionali è la mancanza di personalità giuridica; salvo rari casi, come lo Stato del Wyoming o dello Utah negli USA, le DAO operano come entità "*entityless*", rendendo difficile l'imputazione di responsabilità e la capacità di agire in giudizio; negli Stati Uniti, i casi *CFTC v. Ooki DAO* e *Sarcuni v. bZx DAO* hanno segnato un punto di svolta; a riguardo le Corti hanno stabilito che una DAO può essere citata in giudizio come associazione non incorporata e che i suoi membri possono essere ritenuti responsabili in solido per le obbligazioni assunte o per i danni causati[32].

Il Regolamento (UE) 2023/1114 (MiCAR)[33] rappresenta il primo tentativo sistematico dell'Unione europea di disciplinare i *crypto-asset* e i relativi servizi, incidendo indirettamente sulle DAO in quanto potenziali emittenti o fornitori di servizi di cripto-attività.

MiCAR non contiene una disciplina autonoma delle DAO, ma ne intercetta la rilevanza attraverso la figura dell'"emittente" e dei "prestatori di servizi su cripto-attività", imponendo obblighi di trasparenza, *governance*, gestione dei conflitti e tutela degli investitori.

[31] A. Manganelli, Decentralized Autonomous Organization, blockchain e impresa: considerazioni giuridico-economiche, cit., p. 299.

[32] P. Matera, *Appunti in tema di DAO nell'ordinamento statunitense, Relazione agli Stati Generali del Diritto di Internet e dell'Intelligenza Artificiale*, in *Rivista Diritto di Internet*, 2024; A. Drywleski, *Digital assets and DAOs: new theories of liability*, in *https://www.reuters.com/legal/legalindustry/digital-assets-daos-new-theories-liability-2024-06-10/.*

[33] Il Markets in Crypto-Assets Regulation è il regolamento dell'Unione Europea che introduce un quadro normativo armonizzato per le cripto-attività (Bitcoin, stablecoin, etc.) e i relativi fornitori di servizi, con l'obiettivo di proteggere gli investitori, garantire la stabilità finanziaria e promuovere l'innovazione, definendo regole chiare per l'emissione, la negoziazione e la fornitura di servizi legati a questi asset digitali. Entrato in vigore gradualmente nel 2024-2025, il MiCAR stabilisce requisiti di trasparenza (come i white paper), autorizzazione e supervisione, distinguendo tra le diverse tipologie di token, come gli asset-referenced tokens e gli e-money token. In tema si veda N. De Giorgi, *Regolamento MiCA e disciplina antiriciclaggio (and reverse)*, in *Quaderni di Ricerca Giuridica*, 2025, 103, pp. 147-159.

Cruciale, ai fini delle DAO, è l'art. 2, par. 4 MiCAR, in quanto esclude dal campo di applicazione i *crypto-asset* "emessi in modo completamente decentralizzato, senza l'intervento di un emittente identificabile"; tale clausola di esenzione, formulata in chiave *principle-based*, apre un complesso dibattito interpretativo circa i criteri per qualificare una decentralizzazione come "completa"

Alcuni autori[34] hanno evidenziato il rischio che progetti solo formalmente decentralizzati, ma sostanzialmente controllati da un gruppo ristretto (*founder, core dev*, società di supporto), tentino di sottrarsi agli obblighi MiCAR invocando la clausola di esenzione.

Accanto a MiCAR, il Data Act del 2022 introduce una definizione normativa di *smart contract*, focalizzata sugli aspetti di sicurezza, affidabilità e interoperabilità nell'uso di dati generati da device connessi; la normativa prevede requisiti tecnici, ad esempio meccanismi di "*safe termination*" e controllo dell'esecuzione, che incidono direttamente sulla progettazione degli *smart contract* utilizzati dalle DAO in contesti *data-driven*, imponendo un raccordo più stretto tra logica tecnica e conformità giuridica[35].

Nell'ordinamento italiano non esiste, allo stato, una disciplina organica delle DAO; il principale punto di contatto è rappresentato dal Codice dell'Amministrazione Digitale (CAD, d.lgs. 82/2005), che riconosce validità giuridica al documento informatico e, indirettamente, agli *smart contract*.

L'art. 8-ter del CAD[36], introdotto nel 2019 dal d.lgs n. 235, attribuisce infatti efficacia legale agli *smart contract*, subordinandola al rispetto

[34] F. Di Vizio, *L'abusivismo sollecitatorio rispetto alle criptovalute ai tempi del MiCAR*, in *Il Quotidiano Giuridico*, del 12/01/2026; A. Cesaretti, *DAO e diritto: tra autonomia algoritmica e compliance normativa,* 04/2025 in *https://www.researchgate.net/publication/391194941_DAO_e_diritto__tra_autonomia_algoritmica_e_compliance_normativa*.

[35] S. Siciliano, *Blockchain e smart contracts: aspetti informatico-giuridici,* 7/2022, in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4250342*.

[36] L'articolo riguarda le tecnologie basate su registri distribuiti (Blockchain) e Smart Contract, introducendo definizioni per queste tecnologie, riconoscendo la loro capacità di creare effetti giuridici per la validazione temporale elettronica e prevedendo la loro integrazione nei servizi della Pubblica Amministrazione per la gestione di documenti e processi digitali, come stabilito dal Decreto Legislativo n. 235 del 2019. Questo articolo modernizza il CAD, introducendo ufficialmente la *Blockchain* e gli *Smart Contract* nel quadro normativo italiano per la gestione digitale dei documenti e dei servizi pubblici, conferendo loro valore legale e facilitando la digitalizzazione.

di requisiti tecnici di identificazione delle parti e immodificabilità del codice; ciò consente di ricondurre lo *smart contract* nel paradigma del contratto informatico, ma lascia irrisolto il profilo soggettivo ovvero del "soggetto" che agisce per mezzo della DAO.

La dottrina[37] più attenta alle implicazioni teoriche del fenomeno considera le DAO come "corpi collettivi algoritmici"[38], fondati su una base sociale distribuita, su regole procedurali auto-eseguibili e meccanismi di legittimazione interna basati sulla partecipazione e sulla trasparenza; in questa prospettiva, il diritto non è chiamato solo a comprimere o incasellare le DAO in ambito di categorie esistenti come ad esempio associazioni non riconosciute o società di fatto ma a ripensare le forme della soggettività collettiva in senso più elastico, procedurale e modulare.

In tal senso coloro che rivestono ruoli attivi nella gestione del protocollo, ad esempio detentori di chiavi *multi-sig*[39] o amministratori dei forum di *governance*, potrebbero essere chiamati a rispondere per le attività poste in essere nella DAO, ma il rischio di un'estensione a tutti i *token holder* rimane un'ombra inquietante sulla scalabilità del modello[40].

In questo vuoto normativo il legislatore europeo è chiamato ad intervenire in primis sull'introduzione di un regime opzionale di re-

[37] V. Bellomia, *Il contratto intelligente: profili civilistici*, in *Judicium*, Pacini Giuridica, 2020; M. Durovic - F. Lech, *The Enforceability of Smart Contracts*, in *Italian Law Journal*, 2019, pp. 493-511.

[38] A. Cesaretti, *DAO e diritto: tra autonomia algoritmica e compliance normativa*, 04/2025, in *https://www.researchgate.net/publication/391194941_DAO_e_diritto__tra_autonomia_algoritmica_e_compliance_normativa*.

[39] Rappresentano un sistema di sicurezza per i portafogli di criptovalute che richiede più chiavi private per autorizzare una transazione, distribuendo il controllo e proteggendo gli asset da hacking o errori umani, come ad esempio una cassaforte che necessita di più serrature per essere aperta. In tema si veda P. Eberle, *Crypto Long & Short: Ridefinire lo Standard di Custodia per il Settore Bancario*, in *www.coindesk.com/it/coindesk-indices/2025/11/05/crypto-long-and-short-redefining-the-custody-standard-for-banking*.

[40] O. Borgogno, *Come adattare le Decentralized Autonomous Organizations (DAO) al contesto giuridico*; in Questioni di Economia e Finanza, 2022, 718, pp. 1-22; R. Lener - S. Furnari, *Modelli organizzativi alla prova delle nuove tecnologie. Prime riflessioni su DAO e i principi generali del diritto dell'impresa.*

gistrazione delle DAO, con riconoscimento di personalità giuridica e responsabilità limitata in cambio di requisiti minimi di trasparenza, *governance* documentata e *audit on-chain*; ulteriore intervento auspicabile riguarda la codificazione di criteri positivi di "decentralizzazione effettiva" garantendo l'assenza di *admin keys*[41] unilaterali, una *governance* realmente distribuita, il divieto di promesse di rendimento; tutto ciò per evitare abusi dell'esenzione MiCAR.

È auspicabile, infine, un intervento volto alla elaborazione di un regime di responsabilità graduata, che distingua tra responsabilità dei promotori, dei partecipanti attivi nella *governance* e della DAO registrata, contemperando esigenze di tutela dei terzi e incentivo all'innovazione.

In questa direzione la dottrina italiana e internazionale[42] considera *smart contract e blockchain* come "*regulatory technology*" e le DAO come nuove forme di coordinamento collettivo; a riguardo, le recenti analisi sulle teorie di responsabilità per *asset* digitali e DAO, offrono una base teorica solida di partenza per favorire l'attività del legislatore.

Altro punto di fondamentale importanza per le DAO riguarda la sicurezza informatica, che non è un aspetto meramente tecnico bensì; un requisito ineludibile per la rispettiva efficacia e validità giuridica; se "*the code is law*" ovvero il codice è la legge dell'organizzazione, un difetto nel codice risulterebbe essere un difetto della legge stessa.

Le vulnerabilità del codice possono portare non solo alla perdita di *asset*, ma anche alla paralisi dei processi decisionali o alla manipolazione fraudolenta della volontà collettiva.

[41] In ambito tecnologico e blockchain si riferiscono a credenziali super-potenti, spesso associate a un singolo "autore" (il creatore o il proprietario) o a un DAO, che controllano completamente un sistema (come contratti intelligenti, applicazioni), permettendo modifiche, aggiornamenti o persino la sua chiusura. In tema si veda A. J. Connor, *What are Admin Keys? (Ultimate DeFi Risk)*, in *The Coin Zone*, 2022.

[42] P. De Filippi - S. Hassan, *Technology as a Regulatory Technology: From Code is Law to Law is Code,* in *First Monday*, vol. 21, n. 12, 2016; M. Corrales Compagnucci - M. Fenwick, *Smart contracts: Technological, business and legal perspectives,* in *Bloomsbury Publishing Plc.*, 2021; C. Pongibò, *Dismantling Imaginaries about Smart Contracts*, in *Italian National Reports to the XXIst International Congress of Comparative Law,* ESI, 2022, pp. 741-771.

Le DAO sono esposte a diverse tipologie di *ciber-attak*, ognuna con specifiche implicazioni legali e finanziarie; il report ENISA[43] 2025, basato sull'analisi di quasi 4.900 casi di attacchi informatici, dipinge uno scenario in rapida evoluzione, dove le vulnerabilità vengono sfruttate con una velocità impressionante e gli attori malevoli si fanno sempre più elusivi, evidenziando in tale contesto un aumento significativo delle criticità legate agli *smart contract.*

Mentre gli attacchi al codice colpiscono l'esecuzione, gli attacchi alla *governance*, in particolare, colpiscono la formazione della volontà e quindi del consenso nell'organizzazione decentralizzata delle DAO; l'utilizzazione di *flash loans*[44] permette di acquisire temporaneamente una potenza di voto sproporzionata senza un reale impegno economico a lungo termine; sintomatico a riguardo il caso Beanstalk[45], dove un *hacker* fa utilizzato

[43] Definito anche *Threat Landscape* rappresenta l'analisi annuale dell'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) sulle principali minacce informatiche in Europa; in particolare delinea le minacce più rilevanti e gli attacchi cyber che hanno colpito l'UE mostrando la convergenza tra criminali, Stati e hacktivisti, con il phishing come vettore principale e l'IA che potenzia gli attacchi.

[44] Rappresentano dei prestiti istantanei che fungono sia da strumenti di efficienza finanziaria che da vettori di attacco alla governance delle DAOs; in particolare tali organizzazioni decentralizzate utilizzano i *flash loan* principalmente per ottimizzare la gestione della tesoreria e la liquidità ovvero per eseguire script automatizzati volti a sfruttare discrepanze di prezzo tra exchange (DEX) o liquidare posizioni sotto-collateralizzate, incassando premi per la tesoreria senza immobilizzare capitale proprio; per ristrutturare il debito della DAO, passando ad esempio da un prestito con tassi alti a uno più vantaggioso in un'unica transazione. Chiaramente la duttilità e velocità di tali prestiti viene sfruttata anche per manipolare le decisioni democratiche prese nelle DAO; un utente, ad esempio, può prendere in prestito enormi quantità di capitale per acquistare istantaneamente token di governance, votare una proposta malevola e restituire il prestito nello stesso istante. Cfr. S.L. Furnari, *La finanza decentralizzata. Cripto-attività, protocolli, questioni giuridiche aperte*, Minerva Bancaria, 2023, pp. 175-184; G.L. Comandini, *La Finanza Decentralizzata DeFi:dalle basi all'avanzato: Prestiti e Assicurazioni su blockchain,Yield farming,NFT, Flash Loans*, Hoepli, 2021.

[45] Il caso Beanstalk DAO riguarda un massiccio attacco hacker da 181 milioni di dollari nell'aprile 2022 a un protocollo di stablecoin su Ethereum, dove un hacker ha sfruttato una vulnerabilità della governance (un'improvvisa esecuzione di proposte malevole) tramite un *flash loan*, ottenendo il controllo, svuotando i fondi e facendo crollare il valore della sua stablecoin, Bean, da $1 a $0.10. Secondo la società di blockchain-analytics Elliptic, l'hacker ha preso in prestito circa 1 miliardo di dollari di diverse *stablecoin*, utilizzando un tipo di prestito a brevissimo termine chiamato flashloan, e poi lo ha aggiunto ai fondi di Beanstalk,

un *flash loan* per approvare istantaneamente un trasferimento di circa 182 milioni di dollari dalla tesoreria della DAO al proprio *wallet.*

Lo sviluppatore che redige lo *smart contract* per una DAO assume un'obbligazione che parte della dottrina[46] tende ad inquadrare tra l'appalto di servizi e il contratto d'opera professionale; se il *bug* è prevedibile o deriva da negligenza, il soggetto in questione potrebbe rispondere dei danni arrecati alla DAO e ai suoi investitori.

Si discute, in ambito civile, se tale responsabilità derivi da obbligazione di mezzi (impegno diligente) o di risultato[47] (codice esente da *bug*); alla luce dell'attuale complessità tecnologica, la giurisprudenza[48] propende per un'obbligazione di mezzi aggravata, dove il professionista deve dimostrare di aver adottato tutte le misure di sicurezza allo stato dell'arte.

Sotto il profilo penale, la responsabilità a carico del soggetto che crea e sviluppa uno *smart contract*, ricade spesso nella fattispecie della frode informatica disciplinata dall'art. 640-ter c.p che punisce chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, ovvero intervenendo senza diritto su dati, informazioni o programmi, procura a sé o ad altri un ingiusto profitto con altrui

tutto ciò per ottenere uno schiacciante potere di voto. L'hacker ha poi utilizzato tale potere per approvare la sua idea di donare soldi all'Ucraina; la proposta, al contrario, includeva un codice che invece inviava tutti i fondi bloccati nel protocollo Beanstalk ad un *wallet* (portafoglio) controllato dall'hacker. Una volta "rubati" i fondi, apparentemente seguendo le regole del protocollo, ha ripagato il prestito e intascato la differenza.

[46] Cfr. fra i tanti V. Bellomia, *Il contratto intelligente: profili civilistici*, in *Judicium*, Pacini Giuridica, 2020; S. Cerrato, *Appunti su smart contract e diritto dei contratti*, in *Banca, borsa, tit. cred.,* 2020, 3, pp. 370 ss.; M. F. Tommasini, *Lo smart contract e il diritto dei contratti*, in *Jus Civile*, 2022, 4, pp. 831-862.

[47] Trib. Milano, 6869/2024: In una controversia relativa a malfunzionamenti del software, il giudice ha qualificato la fornitura di software come un'obbligazione di risultato, dichiarando nulla (ai sensi dell'art. 1229 c.c.) ogni clausola contrattuale che limitasse la responsabilità del fornitore per errori o bug critici.

[48] Trib. di Milano, 5091/2024 e 5193/2024; Trib. di Palermo, 1075/2022, tale sentenza pur non riguardando direttamente smart contract, ribadisce che la responsabilità per vizi del software deve essere valutata secondo la diligenza professionale ex art. 1176 c.c., che impone l'adozione di tutte le precauzioni tecniche aggiornate; in dottrina si veda anche L. Rufo - M. Solochewicz, *Blockchain e Diritti: pillole di diritto per la ricerca di un giusto equilibrio*, in *Il potere della tecnica e la funzione del diritto: un'analisi interdisciplinare di blockchain,* a cura di E. Navarretta - L. Ricci - A. Vallini, Giappichelli, 2021, p. 54 ss.

danno; in particolare, in presenza di *criminal smart,* programmati per realizzare operazioni fraudolente come trasferimenti automatizzati di crypto da wallet altrui sfruttando chiavi o accessi non autorizzati oppure di sfruttamento fraudolento di vulnerabilità da parte di un hacker che, manipolando la logica del contratto, ottiene spostamenti patrimoniali indebiti[49] come è capitato a THE DAO nel 2016 vittima di *reentrancy attacks*[50].

3. L'entrata in vigore del *Data Act* ovvero del Regolamento UE 2023/2854 rappresenta una sfida epocale per le DAO che operano nel mercato unico europeo; l'art. 30 del Regolamento introduce "prescrizioni essenziali" per gli *smart contract*, divenute obbligatorie a partire dal 12 settembre 2025.

Il *Data Act* richiede che gli *smart contract* vengano progettati in modo tale da resistere alla manipolazione di terzi prevedendo in particolare meccanismi di "cessazione e interruzione sicura"; tale requisito è noto come *kill switch* ma per una DAO tradizionale sarebbe paradossale; permettere ad uno o piu soggetti dell'organizzazione di poter interrompere il funzionamento della stessa facendo venir meno la decentralizzazione.

La normativa europea sembra, dunque, voler forzare una "ri-centralizzazione" parziale per motivi di sicurezza pubblica e tutela dei consumatori, scoraggiando l'uso di *smart contract* totalmente immutabili e autonomi nelle DAO e in altri particolari settori della *date economy*.

Oltre alla sicurezza, il *Data Act* impone requisiti di interoperabilità e trasparenza, garantendo che i dati gestiti dagli *smart contract* siano

[49] P. Accinni, L'util*izzo criminogeno della blockchain: gli smart contract*, in *SP Sistema Penale*, 2022, 6, pp. 133-148.

[50] The DAO la prima "decentralized autonomous organization" pensata come veicolo d'investimento collettivo governato tramite token, in cui i possessori di token votavano le proposte di investimento, lanciata sulla blockchain di Ethereum nel 2016 come fondo di investimento decentralizzato, fu vittima di un grave attacco basato su una vulnerabilità di *reentrancy* nei suoi *smart contract*. Alcuni hacker riuscirono a sottrarre circa un terzo dei fondi (circa 3,6 milioni di ETH, stimati in circa 60–70 milioni di dollari dell'epoca), provocando una crisi tale da portare al famoso *hard fork* che separò Ethereum da Ethereum Classic.

accessibili e portabili; a riguardo le DAO dovranno dunque prevedere interfacce che permettano agli utenti di esercitare i propri diritti di accesso ai dati, in linea con quanto previsto anche dal *General Data Protection Regulation* (da ora GDPR) in particolare dagli artt. 16 e 17 in tema di diritto all'oblio e alla rettifica[51].

Se una DAO subisce un *data breach* ovvero una violazione della sicurezza che porta all'accesso, alla distruzione, perdita, modifica o divulgazione non autorizzata di dati personali sensibili o riservati, spesso causata da attacchi *hacker*, la conformità normativa diventa tecnicamente impossibile senza un *hard fork*[52] o l'uso di tecniche crittografiche avanzate come le ZKP[53].

A riguardo la giurisprudenza europea[54], incentrata sull'*European*

[51] Alla luce del *Date Act*, per una DAO che tratta dati personali anche solo identificatori onchain "linkabili" ad una persona fisica risulterebbe corretta l'applicabilità dell'art. 17 del GDPR ovvero l'obbligo di prevedere gia nella fase della sua nascita una progettazione *privacybydesign* e procedure di gestione delle richieste di cancellazione che agiscano sull'*offchain* e su chiavi, permessi, accessi (ad esempio revoca di credenziali, delinking tra indirizzi e identità, ritiro di token identificativi, ecc.). In tema si veda R. Grisafi, *Il nuovo diritto di accesso ai dati alla luce del Data Act. Da strumento di protezione della persona a leva di equilibrio del mercato.*, in *Data* Act, in *Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/285*, a cura di A. Morace Pinelli, Pacini Giuridica, 2025, pp. 87-111; G.M. Marisco, *Articolo 17 - Richieste di messa a disposizione dei dati,* in *Data Act. Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/285*, cit., pp. 479-504.

[52] Nello specfico delle DAO trattasi di un aggiornamento radicale del protocollo che crea una nuova catena blockchain, divergendo dalla precedente, spesso per risolvere dispute, aggiungere funzionalità o correggere bug, come nel famoso caso dell'hacking di The DAO su Ethereum nel 2016, che portò alla creazione di Ethereum (ETH) e Ethereum Classic (ETC).

[53] Le Zero-Knowledge Proofs sono tecniche crittografiche avanzate, nelle DAO utilizzate rivestono un ruolo fondamentale in quanto abilitano privacy, scalabilità e fiducia certificando la validità di informazioni (ad esempio chi può votare) senza rivelare dati sensibili come l'identità del votante o i dettagli della transazione; inoltre consentono l'adozione di decisioni anonime ma verificabili, migliorando l'efficienza delle reti blockchain.

[54] La Corte di Giustizia Europea ha emesso diverse sentenze chiave sul trattamento dei dati, chiarendo che i dati pseudonimizzati restano personali se il titolare può reidentificare le persone (sentenza C-413/23, detta "Deloitte"); che le associazioni di consumatori possono intentare azioni rappresentative per violazioni del GDPR, come la mancata trasparenza sulle informazioni, anche senza un mandato specifico dai singoli utenti e indipendentemente dalla prova di un danno concreto per una persona specifica, questo significa che

Digital Identity Wallet, introdotto dal Regolamento eIDAS 2 per gestire identità digitali, documenti personali e accedere a servizi, garantendo sicurezza e controllo utente, sta affrontando sfide su affidabilità, modelli di business e rischi legati a dati sensibili; in particolare, sta valutando se la pseudonimizzazione degli indirizzi *wallet* ovvero il trattamento dei dati in modo che non siano più attribuibili a un individuo senza informazioni aggiuntive, sia, di per sé, sufficiente a escluderli dall'ambito di applicazione del GDPR.

A riguardo, le DAO devono definire chiaramente il titolare del trattamento, gestire i dati in modo lecito, proporzionato e sicuro, garantendo i diritti degli interessati (es. diritto di accesso, opposizione), anche se l'ente non ha personalità giuridica formale.

Recenti sentenze[55] della Corte di Giustizia UE chiariscono che anche entità non formalmente costituite possono essere titolari del trattamento dati, enfatizzando la necessità di chiarezza sui ruoli e il rispetto dei principi di trasparenza e sicurezza, fondamentali in contesti decentralizzati; sembra, quindi, che la giurisprudenza europea stia progressivamente estendendo i principi di protezione dati ai sistemi decentralizzati, inter-

la violazione dell'obbligo informativo del titolare del trattamento costituisce di per sé una violazione dei diritti che può essere oggetto di azione rappresentativa ai sensi dell'articolo 80, paragrafo 2, del GDPR (sentenza C-757/22); che le autorità non possono imporre limiti irragionevoli al numero di reclami che un cittadino può presentare per violazioni della privacy, ribadendo il diritto fondamentale di proporre reclamo a un'autorità di controllo, purché non sia manifestamente infondato o eccessivo. (sentenza C-416/23). Tali decisioni sottolineano che la pseudonimizzazione non esonera dagli obblighi del GDPR se la reidentificazione è possibile, e che la trasparenza e le garanzie sono fondamentali.

[55] CGUE, ottava sezione, sentenza del 27 febbraio 2025 nella causa C-638/23; con tale sentenza la Corte ribadisce che il dettato dell'art.4, punto 7 del GDPR sull'identificazione del "titolare del trattamento" risulta applicabile ad un'entità amministrativa ausiliaria, priva di personalità giuridica, designata direttamente dal diritto nazionale per trattare dati, definendo finalità e mezzi, e stabilendo se tale ente possa essere considerato titolare; CGUE, prima sezione nella causa C-203/22; la Corte si è pronunciata sulla valutazione automatizzata del merito creditizio (credit scoring), con particolare riferimento al diritto dell'interessato ad una spiegazione sulla logica sottesa alla decisione circa la concessione o meno del credito, che gli consenta di comprendere e contestare la decisione automatizzata (così come avviene nelle DAO). Con questa decisione viene stabilito che le informazioni significative devono essere comunicate tramite le autorità di controllo o i giudici nazionali, che ponderano i diritti in gioco, non ammettendo soluzioni definitive predefinite.

pretando il GDPR in modo ampio per garantire tutela, anche se la specificità delle DAO continua a presentare sfide interpretative significative.

Le DAO, in Europa, non godono oggi di una piena e uniforme soggettività giuridica, ma la dottrina e la giurisprudenza stanno progressivamente "riconducendo" il fenomeno entro categorie note come ad esempio associazione non riconosciuta, fondazioni e *partnership*, con rilevanti conseguenze in termini di responsabilità dei partecipanti.

Alcuni autori[56] evidenziano come la DAO priva di veste legale operi in una "*grey area*", priva di personalità, con incapacità di essere parte contrattuale e di far valere diritti in proprio; in Italia, nello specifico, parte della dottrina[57] propone l'introduzione di una categoria speciale di ente per DAO, oppure l'innesto nel diritto delle associazioni/enti del Terzo settore, sottolineando che il nodo centrale è conciliare innovazione, *accountability* e tutela di creditori e utenti.

Ampliando lo sguardo oltreoceano, sulla scia di alcuni casi statunitensi[58], gia citati, la tendenza è quella di negare l'idea della DAO "*enti-*

[56] Cfr. S. Ostrovskiy, *DAO 3.0: Ultimate Legal Structuring for DAOs in 2025 and Beyond,* del 25/02/2025, in *https://aurum.law/newsroom/DAO-3-0-ultimate-dao-legal-structuring-in-2025-and-beyond*; S. Korotana, *Decentralized autonomous organizations: adapting legal structures and proposing a new model of DAOLLP,* in *Capital Markets Law Journal*, Oxford University Press, 2025, 20, 3, pp. 1-11.

[57] S. Ali, *Decentralized Autonomous Organization (DAOs) in Italy: Legal and Regulatory Reforms within the Italian Third Sector (TS) and its effect on Blockchain Innovation*, in *Journal of Ethics and Legal Technologies*, 6, 2024.

[58] I casi Ooki, bZx e Lido segnano il passaggio da DAO "*entityless*" a DAO considerate come soggetti giuridici e aprono alla responsabilità, anche personale, di developer, promotori e tokenholder attivi; in tutti e tre, il nodo centrale è se e come la partecipazione alla governance trasformi i membri della DAO in cotitolari di un'impresa con responsabilità verso terzi. In particolare nel caso Ooki DAO la CFTC (enfocement pubblico) ha agito contro bZeroX LLC (bZx) e poi contro la sua "successor" Ooki DAO per aver offerto leveraged/margined retail commodity transactions in digitale off-exchange, operato come futures commission merchant non registrato e omesso gli obblighi AML/KYC previsti per gli FCM. Il tribunale nel 2023 ha qualificato Ooki DAO come un'associazione non incorporata/persona giuridica ai sensi del Commodity Exchange Act condannandola alla chiusura del sito e a una sanzione pecuniaria di 643.542 dollari. A riguardo si veda K. Brodhel, *The "DAO Jungle" Chronicles: DAO can be Sued as a General Partnership; Token Holders Face Liability*, in *https://thellcjungle.com/2024/12/the-dao-jungle-chronicles-dao-can-be-sued-as-a-general-partnership-token-holders-face-liability/.*

tyless" e di imputare obbligazioni e illeciti o a un *wrapper* legale esterno o direttamente ai membri come cotitolari di un rapporto associativo o para-societario.

La creazione di *legal wrapper* ovvero di entità che possano fungere da "vestito giuridico" per una DAO, conferisce a quest'ultima personalità giuridica, limitazione della responsabilità e capacità di operare nel panorama economico *off-chain*.

Parliamo dunque di una struttura organizzativa tradizionale come ad esempio di un trust o di un'associazione integrata con la *governance* della DAO, così che l'ente possa essere titolare di diritti e obblighi verso terzi; in questo modo una DAO potrebbe stipulare contratti di assicurazione contro *hacker* e furti informatici, riducendo l'impatto finanziario degli *exploit* e designare rappresentanti legali capaci di agire in giudizio in caso di attacco, facilitando il recupero dei fondi tramite procedure legali[59].

Questa soluzione potrebbe permettere ad una DAO, quindi, di essere parte contrattuale, possedere beni e un *Internet Protocol* (IP), aprire conti, agire e resistere in giudizio; in questo modo verrebbero canalizzate attività e relativi rischi in un soggetto con responsabilità limitata, e, di conseguenza protetti i membri dell'organizzazione decentralizzata per le obbligazioni da quest'ultima assunte.

Il futuro delle DAO sembra risiedere in un modello ibrido, dove la decentralizzazione è bilanciata da meccanismi di protezione; l'uso di oracoli non solo per i dati di mercato, ma anche come "arbitri" di sicurezza, potrebbe permettere la sospensione automatica del protocollo in presenza di *pattern* di attacco noti, realizzando quella "interruzione sicura" richiesta dal *Data Act*.

L'analisi condotta evidenzia come l'autonomia algoritmica non possa prescindere da una solida intelaiatura giuridica e da elevati *standard* di sicurezza informatica; le vulnerabilità del codice non sono semplici errori tecnici, ma fonti di rischio legale che possono portare alla rovina

[59] Cfr. V. Villanueva Collao, *Decentralized(?), But Far From Disorganized: A Comparative Analysis of Legal Wrappers and the Evolving Structure of* DAO, in *Social Science Research Network*, del 18/02/2025, pp. 20 e ss.*;* C. Brummer - L. Seira*, Legal Wrappers and DAOs*, in *Social Science Research Network*, 2022.

finanziaria dei partecipanti e alla delegittimazione dell'intero modello decentralizzato.

L'ordinamento europeo, attraverso il *Data Act* e il MiCA, sta tracciando un percorso di regolamentazione che privilegia la sicurezza e la tutela dei diritti fondamentali rispetto alla neutralità tecnologica assoluta; per le DAO, la sfida del prossimo decennio sarà quella di integrare la "*rule of law*" all'interno della "*rule of code*", accettando compromessi sulla decentralizzazione in cambio di una maggiore resilienza e accettazione sociale.

Solo attraverso una cooperazione stretta tra giuristi e sviluppatori sarà possibile costruire organizzazioni che siano realmente autonome, ma anche sicure e legalmente sostenibili nel lungo periodo.

RIFLESSIONI COMPARATISTICHE IN TEMA DI PROTEZIONE GIURIDICA DEL MARCHIO NEL DIGITAL FASHION SYSTEM: OPPORTUNITÀ E NUOVI PERICOLI

Katia Fiorenza

1. Il concetto di marchio affonda le sue radici nell'antichità. Sin dai tempi remoti, artigiani, mercanti e commercianti hanno avvertito l'esigenza di contrassegnare i propri prodotti – mediante l'apposizione di sigilli, simboli e marcature – sia per autenticarne la proprietà, sia per garantirne la qualità. Quest'ultima è stata una delle principali funzioni svolte dalle corporazioni durante il medioevo, i cui statuti, così come gli atti autorizzativi dei Comuni, prevedevano l'impiego obbligatorio del medesimo marchio (o stemma) per coloro che praticavano un'arte[1]. Tale segno era un ineludibile requisito per la commercializzazione del prodotto; da qui l'istituzione della figura dei c.d. funzionari della corporazione, i quali, tra l'altro, avevano l'incarico di sorvegliare il rispetto delle regole imposte dalle singole corporazioni[2].

[1] «Nel Regno Unito, il primo statuto dei marchi in assoluto (la legge sulla registrazione dei marchi) è stato adottato nel 1875. Si racconta che la notte prima del 1º gennaio 1876, data dalla quale è possibile depositare domande di marchio, un dipendente della Bass Brewery, fondata nel 1777, sia stato mandato ad attendere fuori dall'Ufficio dei brevetti per poter depositare la prima domanda di marchio la mattina seguente», in *https://www.euipo.europa.eu/it/news/the-history-of-trade-marks.*

[2] Per un approfondimento storico, cfr. M. Amar, *Dei nomi, dei marchi e degli altri segni e della concorrenza nell'industria e nel commercio*, Utet, 1893; A. Ramella, *Trattato della proprietà industriale*, II, 2ª ed., Unione tipografico - Editrice torinese, 1927, p. 35; M. Ghiron, *Corso di diritto industriale*, II, Edizioni Italiane, 1929, p. 39.

Esistevano diverse forme di marchi, tra cui il marchio collettivo e quello individuale, entrambi obbligatori e volti a garantire la qualità dei prodotti e a proteggere gli interessi delle corporazioni: si poteva risalire al produttore e, in caso di prodotto difettoso, o comunque in contrasto con le prescrizioni di qualità, punire il responsabile. Con l'avvento di una crescente dinamicità economica e sociale e l'abolizione delle corporazioni, a favore della libertà economica individuale, il ruolo del marchio subisce una trasformazione significativa.

La genesi della disciplina dei segni distintivi, che includono il marchio, risale alla Francia liberale. Con la Rivoluzione del 1789 e la conseguente abolizione delle strutture tradizionali – quali le corporazioni medievali –, in contrasto con gli ideali di libertà e competitività, viene avvertita l'esigenza di predisporre un primordiale sistema di tutela, attribuendo all'imprenditore il diritto esclusivo di avvalersi del proprio segno distintivo[3].

La prima legge generale che riconosce il diritto esclusivo all'uso di un marchio si ebbe in Francia nel 1803 e cinquant'anni più tardi viene emanata la legge sui marchi di fabbrica e commercio. Tale disciplina sarà legge del Regno d'Italia nel 1868[4]. Il marchio aveva, e avrà ancora per lungo tempo, un'unica funzione: distinguere i prodotti dell'imprenditore che li aveva messi in commercio e proteggerlo contro contraffattori e imitatori che avessero utilizzato un marchio identico o simile per altri prodotti[5].

La tesi, pressoché dominante in dottrina, si fondava, da un lato, sull'art. 7, lett. *b*, l. 30 agosto 1868, n. 4577, a norma del quale nella

[3] «Si vuole che egli sia riconosciuto e riconoscibile nel mercato per quello che è (…) renderlo responsabile del suo comportamento (…), inoltre si vuole che altri non possano trarre profitto (…), e si tutela così la personalità dell'imprenditore sul mercato». Così, A. Vanzetti - V. di Cataldo, *Manuale di diritto industriale*, 6ª ed., Giuffrè, 2009, p. 4.

[4] Nel 1868 viene promulgata in Italia la prima legge unitaria che disciplina i "marchi e segni distintivi di fabbrica" (l. n. 4577). Il primo marchio registrato sotto la nuova legge (il marchio italiano n. 1) è l'"Olio di Ricino Italiano", così descritto: «Lamina di ottone di forma ottangolare nella cui parte superiore sono scritte in forma semicircolare le parole Olio di Ricino Italiano; sottoposto a queste, vi sono le seguenti: 1 Pressione Extra. Nel mezzo della lastra trovasi un leone che stringe colla zampa destra una spada e l'appoggia sopra un libro aperto (…)».

[5] Sul punto, per una ricostruzione più approfondita, si rinvia a M. Amar, *Dei nomi, dei marchi e degli altri segni e della concorrenza nell'industria e nel commercio*, cit.; M. Ghiron, *Corso di diritto industriale*, II, cit., *passim.*

domanda di brevetto dovevano essere specificati gli oggetti su cui si intendeva apporre il marchio, dall'altro sul "presunto" principio della protezione condizionata alla possibilità di concorrenza[6].

Contestualmente, in ambito internazionale viene emanato uno dei primi Trattati in materia di proprietà industriale e intellettuale, la Convenzione di Parigi del 1883 *per la protezione della proprietà industriale*, i cui principi, ancora oggi rappresentano solide fondamenta del sistema di tutela del marchio: il *principio di assimilazione* (art. 2), in forza del quale i cittadini di ciascuno Stato aderente sono soggetti alle medesime norme e condizioni dei cittadini degli altri Stati membri; il *principio di priorità unionista* (art. 4), che consente a chiunque abbia depositato una domanda per la protezione di un diritto di proprietà industriale (brevetti, marchi, disegni) in uno Stato membro, di presentare entro i sei o dodici mesi successivi una domanda per lo stesso diritto negli altri Stati; infine, la c.d. *protezione "telle quelle"*(art. 6 *quinquies*), che impone ai Paesi aderenti di concedere al marchio una protezione alle medesime condizioni vigenti per la sua valida registrazione nel Paese d'origine.

Particolarmente significativo, sempre nel contesto internazionale, è l'Accordo di Madrid *sulla repressione delle false o fallaci indicazioni di provenienza* (14 aprile 1891)[7] e il successivo accordo per la registrazione internazionale dei marchi riveduto a Stoccolma il 14 luglio 1967, che introduce la registrazione unitaria in luogo del deposito di molteplici domande. Da qui l'istituzione di un registro internazionale dei marchi presso l'OMPI (Organizzazione Mondiale per la Proprietà Intellettuale)[8]; da tale procedura, non origina un marchio unitario dotato di va-

[6] Cfr. P. Greco, *Sui limiti del diritto di esclusiva e su altre questioni in materia di marchi*, in *Riv. dir. comm.*, 1947, II, p. 212 ss. G. De Ruggiero, *Storia del liberalismo europeo*, prefazione di C. Ocone, (1925), Edizioni Società Aperta, 2021, p. 8 s.

[7] Atto riveduto a Washington il 2 giugno 1911, all'Aja il 6 novembre 1925, a Londra il 2 giugno 1934 e a Lisbona il 31 ottobre 1958 II «Qualsiasi prodotto recante una falsa o fallace indicazione di provenienza, nella quale uno dei paesi, cui si applica il presente Accordo, o un luogo situato in uno di essi, fosse direttamente o indirettamente indicato come paese o come luogo d'origine, sarà sequestrato alla importazione in ciascuno dei detti paesi» (art. 1).

[8] Si tratta di una delle agenzie delle Nazioni Unite specializzate nella promozione della protezione della proprietà intellettuale a livello globale, attuata mediante la cooperazione tra gli attuali 193 Stati membri, avente sede a Ginevra.

lidità per tutti gli Stati aderenti, bensì un "fascio di marchi" nazionali, ognuno tutelato in base alla normativa prevista a livello nazionale.

L'OMPI ha adottato un Trattato internazionale denominato "Protocollo di Madrid" (1989), inserito all'interno dell'Accordo di Madrid per la registrazione internazionale dei marchi ratificato in Italia nel 1996 con la legge n. 169 del 12 marzo.

Con tale protocollo viene intensificata la tutela internazionale dei marchi, in particolare si anticipa «il procedimento di registrazione internazionale, disponendo che questa possa aver luogo sin dal momento del deposito della domanda nel Paese di origine, senza dover attendere la registrazione interna», inoltre, per limitare il rischio del c.d. "attacco centrale" «qualora la registrazione sia rifiutata o dichiarata invalida nel corso del quinquennio iniziale essa (*può*) essere convertita una domanda nazionale dotata della priorità originaria»[9].

La registrazione del marchio internazionale è un passaggio chiave per la protezione del *brand*. Il sistema di Madrid, gestito dall'Organizzazione Mondiale della Proprietà Intellettuale (WIPO), consente alle aziende di ottenere protezione del marchio in più Paesi con una singola domanda. Questo sistema semplifica il processo di registra zione e riduce i costi associati. Per registrare un marchio internazionale, l'azienda deve avere una registrazione nazionale o regionale valida. Una volta ottenuta questa, può presentare una domanda di registrazione internazionale attraverso l'Ufficio marchi del proprio Paese, che sarà poi inoltrata alla WIPO[10].

2. A livello europeo, la disciplina dei marchi di impresa si rinviene nella prima direttiva 89/104/CEE del 21 dicembre 1988 recante norme *sul ravvicinamento delle legislazioni degli Stati membri in materia di marchi di impresa*, emanata al fine di conseguire un progressivo adeguamento delle varie leggi nazionali. Tra gli obiettivi principali, oltre all'armonizzazione, vi è quello di dar vita a un sistema volto ad agevolare la

[9] N. Abriani - G. Cottino - M. Ricolfi, *Trattato di diritto commerciale*, *II*, *diritto industriale*, Cedam, 2001.

[10] Così, G. Mongelli, Brand Compliance *nei processi di internazionalizzazione*, in *Fiscalità & commercio internazionale*, 2025, 1, p. 43.

libera circolazione dei prodotti e dei servizi. Tuttavia, la rimozione degli ostacoli – propri della territorialità dei diritti – non si realizzò del tutto, in quanto la protezione dei marchi era profondamente delimitata entro i confini dello Stato in cui era avvenuta la registrazione[11].

La direttiva 2015/2436/UE del 16 dicembre 2015[12] e il Regolamento (UE) n. 2424/2015 *sul marchio di impresa UE*[13] configurano il c.d. "Pacchetto marchi", ossia un intervento normativo significativo predisposto dal legislatore europeo al fine di garantire una più elevata armonizzazione tra gli ordinamenti nazionali e l'ordinamento dell'Unione europea.

Si tratta di una riforma strutturale che si pone quale obiettivo precipuo il rafforzamento dell'efficacia ed efficienza del sistema di tutela in materia di marchi di impresa, attraverso la semplificazione delle procedure inerenti alla registrazione, più accessibile e snella, e una rilevante riduzione dei costi. Tra le novità introdotte si annovera l'abolizione del requisito della rappresentazione grafica, ponendo le premesse per l'estensione della possibilità di registrazione anche ai marchi non convenzionali[14], precedentemente esclusi.

[11] G. Sena, *Il diritto dei marchi. Marchio nazionale e marchio comunitario*, 4ª ed., Giuffrè, 2007, p. 9 ss.

[12] La direttiva 2008/95/CE che sostituisce la direttiva 89/104/CEE, viene abrogata e sostituita dalla direttiva 2015/2436/UE.

[13] Il Regolamento 40/94/CE sul marchio comunitario, adottato dal Consiglio il 20 dicembre 1993, ha avuto il merito di introdurre la figura del marchio unico, sottoposto a una tutela omogenea in tutti i Paesi dell'allora Comunità europea. Il marchio può essere registrato, trasferito, formare oggetto di una rinuncia, di una decisione di decadenza dei diritti del titolare o di nullità e il suo uso può essere vietato soltanto per la totalità della Comunità. (art. 1.2). É prevista, altresì, l'istituzione dell'Ufficio per l'armonizzazione nel mercato interno (UAMI), il quale dal 23 marzo 2016 è stato rinominato Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO). Il Regolamento 40/94/CE, sostituito dal Regolamento 207/2009/CE (e recentemente modificato dal Regolamento 2015/2424/UE) ha introdotto un sistema di protezione del marchio che non si sostituisce a quello offerto a livello nazionale, ma si affianca ad esso, delineando un sistema di tutela parallelo e complementare.

[14] Tali marchi si discostano da quelli tradizionalmente più diffusi, in quanto comprendono elementi quali forme, colori, odori e suoni, e possono essere oggetto di registrazione perché dotati di una sufficiente capacità distintiva. Tra i marchi non convenzionali che vengono ampiamente impiegati nell'industria della moda vi è il marchio a motivi ripe-

Il Regolamento (UE) 2017/1001 *sul marchio dell'Unione europea*, adottato il 14 giugno ed entrato in vigore il 1° ottobre 2017, fornisce la base normativa comune per la concessione del marchio, con validità in tutti i Paesi dell'Unione europea ed estensione automatica anche ai nuovi ingressi «possono costituire marchi UE tutti i segni, come le parole, compresi i nomi di persone o i disegni, le lettere, le cifre, i colori, la forma dei prodotti o del loro imballaggio e i suoni, a condizione che tali segni siano adatti a: a) distinguere i prodotti o i servizi di un'impresa da quelli di altre imprese; e b) essere rappresentati nel registro dei marchi dell'Unione europea («registro») in modo da consentire alle autorità competenti e al pubblico di determinare in modo chiaro e preciso l'oggetto della protezione garantita al loro titolare» (art. 4). La titolarità del marchio può, inoltre, venir meno se diventa denominazione abituale per designare un prodotto o un servizio, in quanto comporta la perdita della sua funzione distintiva.

Alla fine del 2024 è stato pubblicato il nuovo pacchetto legislativo dell'Unione europea in materia di disegni e modelli, che contiene la direttiva (UE) 2024/2823 *sulla protezione giuridica dei disegni e modelli* e il regolamento (UE) 2024/2822. La riforma della disciplina europea del design (il c.d. "design package") nasce con l'obiettivo di semplificare il sistema e renderlo più accessibile ed efficiente[15], snellendo e semplificando le procedure, ma soprattutto aggiornando i fondamenti e l'estensione della tutela, tendendo in considerazione gli sviluppi delle nuove tecnologie[16].

tuti. Si tratta di una tipologia di marchio contraddistinto dalla ripetizione sistematica di un motivo o di un *pattern* sulla superficie di un prodotto. Si pensi al celebre monogramma di *Louis Vuitton* (noto anche come "*Monogram Canvas*") ideato nel lontano 1896 e costituito dalle iniziali "L" e "V" intrecciate e figure floreali e geometriche, disposti secondo una configurazione ordinata e uniforme.

[15] Per un'analisi dottrinale cfr. S. Jacques - E. Derclaye, *The Parody Exception in EU Design law: A Catalyst for Creative Evolution, Innovation and Cultural Discourse*, in *European Intellectual Property Review*, 2024, p. 285 ss.; H. Hartwig, *Evaluation of EU legislation on design protection*, in *Journal of Intellectual Property Law & Practice*, 2022, 2, p. 107 ss.; Id., *The 'Legal Review on Industrial Design Protection in Europe': A closer look*, in *Journal of Intellectual Property Law and Practice*, 2018, 4, p. 332 ss.

[16] Nella Comunicazione della Commissione del 25 novembre 2020, *Sfruttare al meglio il potenziale innovativo dell'UE. Piano d'azione sulla proprietà intellettuale per sostenere la ripresa e la resilienza dell'UE*, si affermava che, «per quanto nel complesso funzionino bene i

L'art. 3 del regolamento (UE) 2024/2822 comprende nella definizione di prodotto qualsiasi oggetto industriale o artigianale, anche se «reso in forma non fisica». L'attenzione della norma è rivolta, quindi, principalmente al mondo digitale e ai suoi elementi. La questione della protezione dei prodotti digitali ha assunto sempre maggiore rilevanza negli ultimi anni in una molteplicità di settori diversi, nei quali un numero crescente di prodotti sono creati in formato immateriale, causando incertezze nell'applicazione di una disciplina pensata per la protezione di prodotti tangibili.

3. Il marchio non rappresenta soltanto un segno distintivo atto a identificare i prodotti o i servizi di un'impresa, ma assolve a una pluralità di funzioni rilevanti dal punto di vista giuridico, economico e sociale. La sua originaria e primaria funzione è sicuramente quella distintiva, ossia la capacità di contraddistinguere, identificandone l'origine imprenditoriale, i prodotti e/o i servizi simili o affini di un'impresa da quelli di altri operatori economici presenti sul mercato. Il carattere distintivo costituisce l'unico requisito ai fini della registrazione: sia la normativa nazionale[17], sia quella europea, stabiliscono che i marchi che difettano del requisito della distintività, non possono essere oggetto

sistemi dei disegni e modelli dell'UE presentano ancora determinate carenze. Le procedure di registrazione sono in parte obsolete e in alcuni casi comportano inutili oneri amministrativi. La protezione delle nuove forme di disegni o modelli (ad esempio disegni o modelli animati, interfacce grafiche utente) non è sufficientemente chiara. Anche la mancanza di chiarezza sulla portata dei diritti relativi a disegni e modelli rappresenta un problema, specialmente in relazione al crescente uso della stampa 3D o alla tutela dei diritti su disegni o modelli in relazione alle merci contraffatte che transitano nell'UE. Infine, in conseguenza dell'armonizzazione solo parziale della protezione dei disegni e modelli in relazione a componenti utilizzati per la riparazione di prodotti complessi, il mercato dei pezzi di ricambio, importante da un punto di vista economico, continua a essere fortemente frammentato, il che provoca una grave distorsione della concorrenza e ostacola la transizione verso un'economia più sostenibile ed ecologica».

[17] La normativa italiana in materia di marchi è disciplinata dal Codice della Proprietà Industriale (c.p.i.), introdotto con il decreto legislativo 10 febbraio 2005, n. 30, e successivamente modificato. L'art. 7 c.p.i. stabilisce che il marchio deve «distinguere i prodotti o i servizi di un'impresa da quelli di altre imprese» e l'art. 13 c.p.i. ribadisce che «non possono costituire oggetto di registrazione come marchio d'impresa i segni privi di carattere distintivo».

di registrazione. Tale funzione è nota anche, nel diritto anglosassone, come "*Badge of origin*", ossia il marchio opera come indicatore essenziale dell'origine imprenditoriale.

Il marchio è un segno distintivo che consente di differenziare i beni o i servizi di un'impresa da quelli offerti dalla concorrenza. Attraverso il marchio, i consumatori vengono posti in condizione di riconoscere l'origine imprenditoriale di un determinato bene selezionando in modo consapevole il prodotto ritenuto migliore in termini di qualità e/o prezzo e di affidabilità. In tal modo, esso non solo favorisce una maggiore trasparenza sul mercato, ma rappresenta un elemento di intermediazione tra produttore e consumatore, rafforzando reciprocamente la fiducia e contribuendo in modo determinante alla costruzione della reputazione commerciale dell'impresa.

Il messaggio veicolato dal marchio può estendersi anche a qualità ulteriori e immateriali, divenendo espressione di valori che riflettono idee prestigio, esclusività e tradizione. Attraverso la forza attrattiva e la capacità distintiva, il marchio genera delle suggestioni che trascendono il bene fisico, trasformando l'acquisto in *reputation capital*. A tal proposito la dottrina anglosassone discorre di *brand equity*, ossia valore aggiunto che scaturisce dalla percezione collettiva di un marchio e dal significato che esso assume nel contesto sociale e culturale. Il marchio diviene dunque un *asset* strategico delle imprese, capace di generare fiducia e fedeltà[18]. Ed è proprio la capacità evocativa a conferire al marchio il c.d. *selling power*: il consumatore non acquista un prodotto, ma anche ciò che esso rappresenta[19].

Dalla funzione distintiva discende, in capo al titolare del marchio registrato, un diritto di esclusiva che, tuttavia, non è fine a sé stessa

[18] Sul punto v. J.B. Swann - T.H. Davis Jr., *Dilution, An Idea Whose Time Has Gone; Brand Equity As Protectable Property, The New/Old Paradigm*, in *The Journal of Intellectual Property Law*, 1994, 1, 2, p. 238: «many tradermarks are no longer mere words indicating source but are symbols with indipendent value and are entitled to be protected like any other corporate asset».

[19] C. Galli, *Il marchio come segno e la capacità distintiva nella prospettiva del diritto comunitario,* in *Dir. Ind.*, 2008, p. 425 ss. L'a. ritiene che il marchio, con la sua capacità di evocare immagini gratificanti per l'acquirente del prodotto o del servizio contraddistinto dona al prodotto un valore aggiunto rilevante per il pubblico.

ma trova giustificazione nella necessità di assicurare l'effettività della funzione distintiva e di tutelare, altresì, il consumatore da pratiche fuorvianti. Il marchio assume dunque una duplice dimensione: da un lato assurge a strumento di identificazione commerciale, dall'altro rappresenta una forma di tutela giuridica che si fonda non soltanto sull'interesse privato del titolare, ma anche sulla più ampia esigenza di corretto funzionamento del mercato.

4. È certamente tempo di riconoscere che la rivoluzione digitale in corso da alcuni decenni, e fortemente accentuatasi proprio negli ultimi due lustri, pone il tema oggetto di analisi di fronte a un cambiamento epocale legato a un'ipertrofica produzione di massa nel cui ambito si delinea la possibilità per i consumatori di scegliere tra un'ampia varietà di beni provenienti da diversi produttori. Una scelta che può essere veramente consapevole soltanto se guidata dalla presenza di un marchio associato alla fiducia, alla qualità, all'innovazione e alla affidabilità[20].

La trasformazione digitale costituisce una delle principali sfide per l'economia contemporanea, sia per la sua incidenza trasversale in ogni settore produttivo, sia per la sua capacità di indurre verso una ridefinizione sostanziale dei modelli organizzativi e delle dinamiche di mercato. Le innovazioni che ne conseguono consentono il superamento dei tradizionali limiti geografici e l'accesso a nuovi mercati, divenendo un fattore strategico di competitività, caratterizzato da un approccio agile e dinamico, in grado di ridefinire il settore della moda sotto il profilo dell'efficienza operativa, della sostenibilità e nella relazione stessa con i consumatori[21].

Attraverso il digitale, la moda diventa sempre più accessibile e globalizzata, contribuendo non soltanto alla diffusione capillare di marchi e prodotti, ma anche a un ampliamento del mercato e a una diversificazione dei canali di vendita. «Digitization is transforming the way firms

[20] V., in proposito, N. Abriani - G. Cottino - M. Ricolfi, *Diritto industriale*, cit., p. 22.

[21] V. Jacometti, *Diritto e moda sostenibile tra iniziative legislative e iniziative volontari*, in Fashion Law. *Le problematiche giuridiche della filiera della moda*, a cura di V. Jacometti - B. Pozzo, Giuffrè, 2026, p. 341 ss.

across many industries operate. By converting analogue information into digital data, companies are able to access and process information more quickly and efficiently»[22], la tecnologia digitale ha reso possibile lo sviluppo di nuovi materiali e tessuti più sostenibili rispetto a quelli tradizionali che assieme a tempi di produzione più rapidi e migliori processi di controllo garantiscono prodotti di maggiore qualità e a costi inferiori[23].

Nel settore della moda sono mutate le modalità di comunicazione, di produzione e di commercializzazione dei prodotti e introdotte innovazioni significative che impattano sulla gestione dei processi aziendali e sulle relazioni con i consumatori[24]. Si pensi a come l'esplosione dei social media abbia determinato un ripensamento delle strategie comunicative, favorendo l'interazione tra i *brand* e i consumatori, mediante approcci in grado di garantire un coinvolgimento costante del pubblico di riferimento, quali lo *storytelling* e la narrazione del marchio.

Accanto alle nuove modalità di comunicazione attraverso le pagine social si diffondono sempre più le app proprietarie dei singoli marchi, che consentono – oltre alla normale visualizzazione del catalogo e all'acquisto del prodotto – esperienze digitali più avanzate (già nel 2018 Gucci grazie alla "realtà aumentata" permetteva di visualizzare gli item della collezione della Maison in spazi reali). Un settore potenzialmente in grande espansione, in quanto le app funzionano sempre più come esperienze emozionali globali, che accompagnano la possibilità

[22] B. Rathore, *Fashion Transformation 4.0: Beyond Digitalization & Marketing in Fashion Industry*, in *Euduzone International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ)*, 2021, 10, 2, p. 54 s.

[23] Il digitale modifica profondamente quelli che erano i mestieri tradizionali della moda: piattaforme come CLO 3D permettono di sviluppare in digitale tutte le fasi della produzione sartoriale, generando un deciso miglioramento in termini di sostenibilità: è possibile procedere per prove ed errori, progettando e scartando virtualmente forme e modelli senza sprecare materiali spesso preziosi e di forte impatto ambientale. V., in argomento, G. Lunghi, Tecno-Fashion: *moda e trasformazione digitale*, in *Culture Digitali*, 2023, *https://www.diculther.it/rivista/tecno-fashion-cosi-la-moda-e-termometro della-trasformazione-digitale/*.

[24] Per una ricostruzione di ampio respiro sul tema, v. Fashion Law. *Le problematiche giuridiche della filiera della moda*, a cura di V. Jacometti - B. Pozzo, cit.

di acquisto con varie modalità di intrattenimento, personalizzazione, informazione, spettacolarizzazione.

L'adozione di strategie digitali contribuisce, *in primis*, alla costruzione di una immagine positiva del *brand*[25] e, in secondo luogo, al consolidamento del rapporto di fiducia con la clientela, fattori che determinano un notevole incremento delle vendite.

Assistiamo dunque a una trasformazione radicale nel settore della moda. Il ruolo centrale rivestito dai social media emerge dalla constatazione che piattaforme digitale quali *Tik Tok*, *Facebook*, *Youtube* e *Instagram* hanno modificato le modalità attraverso le quali i *brand* comunicano ai consumatori, promuovono i loro prodotti e influenzano le scelte d'acquisto[26]. In tale contesto, il diritto si rivela necessario per fornire strumenti capaci di bilanciare l'innovazione con la tutela degli interessi pubblici e privati coinvolti, garantendo certezza giuridica e protezione adeguata a soggetti economici sempre più esposti ai rischi derivanti dalla digitalizzazione.

5. La ridefinizione dei paradigmi operativi inerenti all'utilizzo degli strumenti digitali ha determinato il sorgere di questioni giuridiche di rilievo riguardanti l'emersione di fenomeni illeciti. Il rapido sviluppo delle tecnologie digitali e la diffusione estesa del commercio *online* hanno profondamente inciso sul mercato della moda, offrendo ulteriori opportunità, ma al contempo nuove sfide in termini di proprietà intellettuale. La tutela di quest'ultima, con specifico riferimento ai marchi, risulta una delle sfide attuali più complesse, in considerazione della notorietà e dell'elevato valore commerciale di cui sono contraddistinti.

[25] N. Ahmad - A. Salman - R. Ashiq, *The Impact of Social Media on Fashion Industry: Empirical Investigation from Karachiites*, in *Journal of Resources Development and Management*, 2015, vol. 7, p. 2: «Social media has become one of the most popular fashionable tools which creates link between brand and the consumer. This link not only gives boost to the purchase intent but it also increases the oral communication. In addition to this social media can be very helpful in projecting the brands image in the minds of well informed and conscious consumers».

[26] P. Bhonsle - N. Soni - C. Mohan, *Fashion in the Digital Age: Social Media Marketing's Influence on the Apparel Market*, in *Shodhkosh: Journal of Visual and Performing Arts*, 2024, p. 1131 s.

5.1. Nel contesto digitale contemporaneo, il nome a dominio assume un valore strategico per i marchi che operano nel settore della moda. L'espressione *domain name* indica una serie di stringhe alfanumeriche, separate da punti, che consentono di identificare in modo univoco un sito web su Internet. La comunicazione tra dispositivi connessi in rete avviene mediante il Protocollo Internet (IP), il quale assegna a ciascun terminale un indirizzo numerico univoco strutturato in sequenze. In ragione della scarsa praticità di tale meccanismo, nel 1983 gli informatici Paul Mockapetris, Craig Partridge e Jon Postel svilupparono il *Domain Name System*, un sistema gerarchico in grado di convertire gli indirizzi IP in termini facilmente memorizzabili per gli utenti, rendendo l'accesso ai contenuti web più agevole e intuitivo[27].

Per i *brand* del *fashion system* il dominio non svolge una mera funzione tecnica, bensì assume un valore identitario in cui l'immagine, il posizionamento e la riconoscibilità sono cruciali. In tal senso, l'utilizzo di un dominio corrispondente al marchio (es. www.armani.com), si configura come un'effettiva estensione digitale del marchio in quanto consente di garantire, non soltanto un accesso agevolato per il pubblico, ma anche di rafforzare l'associazione mentale intercorrente tra il nome e il prodotto, riducendo contestualmente il rischio di confusione[28].

Cybersquatting, neologismo inglese che unisce la radice di "cibernetica" al verbo "to squat", significa occupare abusivamente una casa e descrive efficacemente un fenomeno di accaparramento di chi occupa uno "spazio digitale" appartenente ad altri per trarne vantaggio economico

[27] S. Martinelli, *La disciplina dei nomi a dominio e i rimedi esperibili in caso di cybersquatting*, in *Riv. int. inf. giur*., 2015, vol. 16, n. 54, p. 405 ss.

[28] L'ordinanza del Trib. Milano, 16 maggio 2003, n. 28691, costituisce una chiara espressione e conferma dell'orientamento giurisprudenziale italiano (ormai consolidato) che pacificamente applica i principi della disciplina dei segni distintivi anche ai *domain names*, considerandoli alla stregua di segni distintivi di fatto atipici. Tra le più significative pronunce si segnalano: Trib. Pescara, 9 gennaio 1997, in *Dir. inf*., 1997, p. 952 (caso Nautilus); Trib. Milano, 22 luglio 1997, *ivi*, p. 957 (caso Amadeus); Trib. Roma 2 agosto 1997, *ivi,*1997, p. 961 (caso Porta Portese); Trib. Napoli, 8 agosto 1997, in *Giust. civ.*, 1998, p. 259; Trib. Verona 25 maggio 1999, in *Foro it.*, 1999, I, c. 3061 (caso Technovideo); Trib. Genova 17 luglio 1999, in *Dir. inf*., 2000, p. 346 (caso Altavista); Trib. Prato, 19 agosto 2000, in *Riv. dir. ind.*, 2002, p. 51; Trib. di Firenze, 29 giugno 2000.

o reputazionale[29]. Si tratta di un fenomeno denominato anche *domain grabbing* che consiste nella registrazione abusiva di nomi di dominio corrispondenti a marchi altrui, più precisamente noti o di elevata riconoscibilità, al fine di trarne un vantaggio economico.

Trattasi di una pratica frequente nell'ambito della moda, dove la capacità evocativa del marchio assume una centralità che investe la sfera commerciale e reputazionale. La condotta del c.d. *cybersquatter* si fonda sull'applicazione del principio del «*first come, first served*»[30] che è posto alla base del sistema di registrazione dei nomi a dominio a livello globale[31]. Tale criterio prevede che l'assegnazione del *domain name* avvenga a favore del soggetto che ne faccia richiesta in via prioritaria e automatica, indipendentemente dall'eventuale titolarità di diritti anteriori su quel determinato nome.

Nel corso degli anni, l'evoluzione del fenomeno ha evidenziato un costante incremento della sua complessità, favorita dalla facilità di registrazione dei domini e dall'assenza di controlli preventivi in merito al procedimento di registrazione di un nome a dominio, principale elemento di differenziazione rispetto alla procedura di registrazione di un marchio, il quale implica invece una fase istruttoria con verifiche formali e sostanziali.

[29] Cfr. S. Vitrò, *Il fenomeno del* cybersquatting *e la tutela del nome a dominio*, Giappichelli, 2021, p. 31 ss.; A. Fittante, *La rilevanza del nome a dominio ed il conflitto con i marchi e gli altri segni distintivi*, in *Il diritto industriale*, 2018, 1, p. 88.

[30] Tale regola, se da un lato ha favorito la rapida diffusione di Internet, dall'altro ha reso vulnerabile il sistema di assegnazione dei *domain name*, aprendo la strada agli abusi da parte di soggetti privi di titoli giuridici legittimi. In argomento v., ampiamente, S. Vitrò, Domain Names: *dal* cybersquatting *alla contraffazione online*, Key Editore, 2019.

[31] Secondo l'Organizzazione Mondiale della Proprietà Intellettuale nel 2023 sono state presentate oltre 6000 denunce di *cybersquatting*: un aumento di quasi il 10% rispetto all'anno precedente, che arriva a superare il 60% se paragonato ai dati di cinque anni fa. Il *combosquatting* rappresenta la più pericolosa tra le varianti del *cybersquatting* e da una ricerca svolta nel 2022 (N. Aizenberg, *DNS Cybersquatting: The Case for Edge DNS Zone Protect*, consultabile su https://www.akamai.com/blog/security/dns-cybersquatting) è emerso che a essere più frequentemente aggiunti ai nomi di dominio sono parole come *"verification"*, *"alert"* o *"security"*, all'evidente fine di sfruttare il senso di urgenza che tali parole suscitano negli utenti.

Il *cybersquatting* si manifesta in una pluralità di varianti (ognuna con caratteristiche specifiche) che sfruttano le falle del sistema di assegnazione[32].

Un'evoluzione subdola e sofisticata delle pratiche illecite online correlate all'abuso del marchio è rappresentata dal c.d. *typosquatting*[168], condotta sempre più diffusa e insidiosa che consiste nella registrazione di nomi di dominio volutamente simili a quelli di marchi noti, ma che presentano alterazioni che sfruttano gli errori di digitazione o di ortografia da parte degli utenti (es. «*pradaa.com*» invece di «*prada.com*»). Nell'ambito della moda, caratterizzata da un'elevata riconoscibilità dei marchi e da un elevato impatto comunicativo, tale fenomeno si rivela particolarmente pericoloso. Esso rappresenta una minaccia concreta in un contesto in cui il valore del marchio è strettamente correlato all'identità digitale. Di conseguenza, anche modifiche minime nella composizione ortografica del nome a dominio possono risultare idonee a generare confusione tra i consumatori, compromettendo la reputazione del *brand*.

Emblematico è il caso deciso nel 2022 dalla *WIPO Arbitration and Mediation Center*[33], inerente al dominio «*top.fashionova.com*» registrato da un soggetto privo dell'autorizzazione della società titolare del marchio, che si è avvalso di un servizio di protezione della privacy denominato *Withheld for Privacy*. La società statunitense *Fashion Nova*, *leader* nell'*e-commerce* dell'abbigliamento, titolare di vari marchi – registrati non soltanto negli Stati Uniti – tra i quali *Fashion Nova* e *Fa-*

[32] Per citarne alcune: il *domain grabbing* che consiste nel registrare come nome a dominio il segno distintivo o il nome di un soggetto terzo – spesso particolarmente noto o riconoscibile – con l'unico scopo di appropriarsi della notorietà associata a quel segno (A. Fittante, *La rilevanza del nome a dominio ed il conflitto con i marchi e gli altri segni distintivi*, cit., p. 96); il *typosquatting* che sfrutta errori tipografici o variazioni minime nel nome di dominio per ingannare gli utenti (es. cybersecurlty.it anziché cybersecurity.it); il *punycode* che rappresenta la forma più sofisticata del *typosquatting* in cui i caratteri speciali (come lettere accentate) sono sostituiti da sequenze di caratteri simili, creando un dominio visivamente simile ma tecnicamente diverso dal dominio originale. Questi domini sono spesso utilizzati per attività *phishing* (M. Cuscusa, Cybersquatting: *cos'è e come difendersi dal furto di domini Web*, in *https://www.cybersecurity360.it.*).

[33] WIPO, 20 luglio 2022, *Fashion Nova, LLC, v. Privacy service provided by Withheld for Privacy ehf /harry trans*, n. D2022-2028, in *https://www.wipo.int/amc/en/domains/decisions/pdf/2022/d2022-2028.pdf.*

shionnova.com. Attraverso campagne pubblicitarie e collaborazioni con celebrità aveva consolidato una consistente presenza online e costruito una rilevante reputazione. Il dominio contestato riproduceva il marchio con una minima variante ortografica (consistente nella rimozione della seconda lettera «*n*» in «*fashionnova*» preceduta da un termine estremamente generico, ossia «*top*») la quale è stata espressamente qualificata dal *panel* come manifestazione di t*yposquatting*, in quanto determinava un dominio simile al marchio originale, sfruttando un errore di digitazione frequente da parte del pubblico. Il sito collegato al dominio era altresì strutturato in modo pedissequo al sito ufficiale della società statunitense, generando confusione nel consumatore medio. In considerazione di tali elementi, il *panel* ha evidenziato che l'intento del registrante era quello di trarre profitto dalla notorietà del marchio e di indurre gli utenti nell'erronea convinzione che si trattasse di un sito ufficiale o comunque affiliato. La vicenda si è conclusa con la riassegnazione del dominio al legittimo titolare del marchio.

Negli Stati Uniti l'*Anti-Cybersquatting Consumer Protection Act* (ACPA), legge federale del 1999, fissa la cornice legale entro cui affrontare questi fenomeni, mentre la *Uniform Domain Name Dispute Resolution Policy* (UDRP) – definita dall'*Internet Corporation for Assigned Names and Numbers* (ICANN) – stabilisce una procedura extra-giudiziaria per mitigarne gli effetti. L'ACPA vieta la registrazione, l'utilizzo o la vendita di nomi di dominio che violino intenzionalmente i diritti di marchio di un'azienda o di un'organizzazione. Le vittime di *cybersquatting* possono intentare una causa civile e ottenere il trasferimento del nome di dominio indesiderato e chiedere il risarcimento di potenziali danni economici[34]. È prevista una responsabilità aggravata per il registrante di un dominio identico o confondibile rispetto a un marchio altrui, qualora agisca con *bad faith intent to profit*. La legge federale statunitense consente la condanna al trasferimento del dominio e al pagamento di *statutory damages* fino a 100.000 dollari per ciascun nome

[34] Nel 2018 *Coca Cola* ha affrontato numerosi casi di *cybersquatting*, oltre cento nomi di dominio registrati da terze parti contenenti il marchio *Coca Cola*. Attraverso l'applicazione dell'ACPA e la collaborazione con i registri di domini, l'azienda è riuscita a ottenere il trasferimento della maggior parte di tali nomi di dominio indesiderati.

a dominio, con un apparato sanzionatorio notevolmente più incisivo rispetto alle tipiche azioni civilistiche europee[35].

L'UDRP, a sua volta, stabilisce una procedura amministrativa per la risoluzione di controversie relative ai nomi di dominio offrendo alle aziende vittime di *cybersquatting* un meccanismo più rapido ed economico per recuperare il controllo dei propri nomi di dominio, senza far ricorso alle vie giudiziarie.

Con riferimento al contesto giuridico italiano, il d.lgs. n. 30/2005[36] ha riunito in un unico *corpus* normativo la disciplina inerente a diversi istituti, tra i quali marchi, disegni, modelli e brevetti. La scelta riflette l'esigenza di assicurare una trattazione logica, ordinata e conforme della materia, garantendo, ad un tempo, l'adattamento legislativo alle disposizioni normative europee e internazionali. Nel corso degli anni il nostro legislatore è intervenuto più volte fino a introdurre con la legge del 24 luglio 2023, n. 102, una importante riforma volta a rafforzare la competitività italiana e a semplificare, anche attraverso la digitalizzazione, le procedure amministrative.

Tuttavia, sebbene il legislatore italiano non abbia introdotto una normativa specifica sul *cybersquatting*, l'ordinamento dispone di strumenti efficaci che consentono di reprimere tali condotte attraverso un sistema combinato di disposizioni penalistiche, civilistiche e di diritto industriale. L'articolo 640 c.p. prevede che chiunque, con artifizi o raggiri, procuri a sé o ad altri un ingiusto profitto a danno di terzi, può essere accusato di truffa. Tale disposizione può senz'altro essere applicata ai casi di *cybersquatting*, in quanto pratica spesso finalizzata a ottenere un guadagno illegittimo, ad esempio attraverso la rivendita del dominio a prezzi esorbitanti.

Il *cybersquatting* può configurarsi quale violazione dei diritti di proprietà industriale, visto che l'uso di un dominio corrispondente a un marchio registrato può indurre confusione tra i consumatori e danneggiare l'immagine dell'azienda legittima. Chi subisce uno *squatting* dei

[35] A. Ashiru, *Criminalisation of Cybersquatting in Nigeria, England and the United States: an Unusual Coexistence of Criminal Law and Intellectual Property right*, in *Journal of legal studies and research*, vol. 7, n. 1, 2021, p. 165 ss.

[36] Il d.lg. 10 febbraio 2005, n. 30, *Codice della proprietà industriale, a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273*, è entrato in vigore il 19 marzo 2005.

domini può richiedere l'intervento legale per ottenere la riassegnazione del dominio e il risarcimento dei danni subiti.

Il Codice del consumo (d.lgs. n. 206/2005) fornisce ulteriori strumenti di tutela per i consumatori. Quando i *cybersquatter* utilizzano domini che sfruttano marchi registrati o nomi noti per ingannare i clienti e condurli su siti fraudolenti, si può configurare una violazione delle norme contro le pratiche commerciali scorrette. Le autorità competenti, come l'AGCM (Autorità Garante della Concorrenza e del Mercato), possono intervenire e sanzionare i responsabili di tali illeciti. È altresì possibile fare ricorso alla procedura di riassegnazione dei domini presso il Registro.it, l'organismo che gestisce i nomi di dominio con estensione ".it". Tale procedura consente ai titolari di marchi o nomi legittimi di ottenere il trasferimento del dominio contestato, qualora sia dimostrato che è stato registrato in malafede o senza un legittimo interesse da parte del *cybersquatter*.

Il quadro normativo italiano offre dunque una serie di strumenti per combattere il *cybersquatting* e proteggere i diritti dei titolari di marchi e dei consumatori, garantendo al contempo un mercato digitale più sicuro e trasparente.

5.2. Dall'analisi del quadro giuridico del *cybersquatting*, è facile intuire che tale condotta illecita sia particolarmente frequente e assolutamente dannosa per i *brand* del lusso, abituati a intrattenere un numero elevato di relazioni commerciali attraverso le proprie piattaforme *online*. Aziende molto importanti, del calibro di *Louis Vuitton, Hermès, Armani*, *Nike* e *Apple*, sono state vittime di *cybersquatting*.

Un caso emblematico in tema di *cybersquatting* nel settore della moda è rappresentato dalla vicenda che ha coinvolto la celebre *maison* italiana Armani[37]. La controversia è scaturita a seguito della registrazione nel 1997 del *domain name* «*www.armani.it*» da parte del titolare di un timbrificio di Treviglio che aveva legittimamente utilizzato il proprio cognome per identificare il proprio sito internet. Il 22 ottobre 1998 Luca Armani è stato citato in giudizio dalla *Giorgio Armani S.p.A.*, la

[37] Trib. Bergamo, sez. civile, 3 marzo 2003, n. 0634, *Giorgio Armani S.p.A. c. Armani Luca*.

quale lamentava una lesione del diritto all'uso esclusivo del marchio. La società attrice sosteneva che l'utilizzo del dominio contestato, identico al marchio registrato e ampiamente riconosciuto, potesse indurre il pubblico a ritenere che il sito fosse attribuibile alla *maison*, che già vantava un'esperienza pluriventennale nel comparto della moda e un posizionamento di primaria importanza in ambito nazionale e internazionale. In considerazione di ciò, la *Giorgio Armani S.p.A.* evidenziava che un utente medio alla ricerca del sito ufficiale della casa di moda, avrebbe ragionevolmente digitato «armani.it» presumendo, sulla base della notorietà del marchio, di accedere al sito istituzionale della società milanese. Ne derivava che l'utilizzo di tale dominio da parte del convenuto avrebbe indotto in errore i consumatori e generato un concreto rischio di confusione tra le due aziende, in quanto l'utente sarebbe stato indirizzato su una pagina web riconducibile a un'attività totalmente estranea alla moda.

L'attrice invocava l'applicazione degli artt. 1 e 13 della legge marchi sussistendo i requisiti richiesti ai fini della tutela del marchio rinomato, ossia un indebito vantaggio e un pregiudizio[38]. La *maison*, inoltre, deduceva la violazione dell'art. 2598 c.c., in quanto la condotta del convenuto risultava astrattamente riconducibile alla fattispecie di concorrenza sleale per confondibilità tra segni distintivi e per sfruttamento parassitario dell'altrui rinomanza.

Il convenuto, eccependo l'infondatezza della domanda, negava che il *domain name* potesse essere qualificato come segno distintivo, trattandosi piuttosto di un mero indirizzo funzionale a individuare un sito web. Sosteneva, altresì, la non configurabilità della contraffazione, avendo utilizzato in modo legittimo il proprio cognome come nome a dominio, in assenza di finalità parassitarie. Analogamente, contestava la sussisteva dell'illecito ai sensi dell'art. 2598 c.c., in quanto le attività svolte dalle parti erano radicalmente differenti.

In assenza di una disciplina legislativa espressa in materia, il Tribunale attraverso un'interpretazione analogica, rileva che il nome a dominio, formato da più componenti, una parte iniziale comune consistente

[38] Artt. 1 e 13, R.D. 21 giugno 1942, n. 929 applicabili *ratione temporis* ai fatti oggetto di causa, successivamente abrogati e sostituiti dagli artt. 20 e 21 del d.lgs. n. 30/2005.

nella dicitura «*http://www.*», una parte finale indicativa dell'estensione geografica («*.com*» o «*.it*») e una parte centrale distintiva, svolge una funzione essenziale nell'identificazione di un sito web. Per tale motivo, non può essere considerato un mero indirizzo tecnico, bensì un segno distintivo, in grado di attrarre gli utenti, invogliandoli a visitare il sito web, adempiendo a una funzione di identificazione commerciale analoga a quella dei marchi.

Nel caso di specie, il nome a dominio oggetto della controversa era utilizzato dall'impresa individuale per promuovere prodotti e servizi di natura commerciale, assumendo a tutti gli effetti la funzione di segno distintivo e, pertanto, assoggettabile alle norme sulla tutela dei marchi. Considerata, inoltre, la natura di marchio celebre attribuita alla storica *maison*, viene riconosciuta una protezione più estesa che impedisca a terzi di trarre indebitamente vantaggio dalla valenza attrattiva del marchio in parola. Il Tribunale di Bergamo riconosce dunque la fondatezza delle ragioni avanzate da *Giorgio Armani S.p.A.*

È, tuttavia, doveroso precisare che tali condotte illecite non rappresentano un pericolo esclusivamente per *brand* molto potenti o affermati da tanti anni nel panorama economico mondiale, il *cybersquatting* costituisce un rischio anche per imprese di piccole e medie dimensioni e relativamente nuove sul mercato. Si pensi all'azienda francese *Jacquemus*, marchio del lusso parigino, che grazie alle mini-borse *"Chiquito"*, cappelli *oversize* di paglia *"Le Grand Chapeau Valensole"* e a fan famosi quali Bella Hadid e Kim Kardashian, ha avuto una crescita esponenziale negli ultimi anni. Inevitabilmente tutto ciò ha attirato l'attenzione dei *cybersquatters*, al punto che il marchio del lusso, attraverso il team legale, ha dovuto difendere il proprio nome e la reputazione con diversi procedimenti.

L'OMPI ha ordinato che molti nomi a dominio, contenenti il marchio *"Jacquemus"* e non appartenenti all'azienda di moda parigina, fossero trasferiti dagli utenti, che li utilizzavano in malafede al fine di confondere i consumatori, alla *maison* francese. Nel caso n. D2020 – 2073, *Jacquemus SAS v. Wenben Zhou*, l'OMPI riconosce che il convenuto cinese ha registrato in data 4 maggio 2020 il nome a dominio *"fashionjacquemus"*, molto simile al marchio della ricorrente (*Jacquemus*).

Tale *domain name* riportava a un sito contenente prodotti simili a quelli di *Jacquemus*, ma a prezzi estremamente ridotti, riproducendo anche immagini del sito *web* originale, senza il consenso del denunciante. Viene riconosciuta anche la mancanza di diritti o interessi legittimi del resistente cinese in relazione al nome a dominio contestato, non avendo il ricorrente autorizzato, concesso in licenza o altrimenti consentito al resistente di utilizzare il marchio in questione e non avendo l'azienda parigina alcun tipo di rapporto commerciale con il convenuto cinese. L'utilizzo in malafede è stato provato considerando l'utilizzo di immagini appartenenti al sito *web* della casa di moda parigina e i prodotti contraffatti. Il pericolo di confusione per il consumatore viene spiegato dagli esperti, attraverso diversi studi di settore, come un fenomeno chiamato *invisible trademark infringement*: l'utente è portato, a causa di un'associazione mentale di idee, a ritenere che il convenuto, nel caso di specie l'utente cinese, produca gli stessi prodotti della *maison* francese o, perlomeno, prodotti che abbiano caratteristiche simili a quelle dei beni prodotti dalla stessa, inducendo così il consumatore alla confusione sopracitata.

6. Negli ultimi anni, si è registrato un incremento allarmante del fenomeno della contraffazione, ossia la produzione di beni realizzati illegalmente che riproducono in modo ingannevole le caratteristiche di quelli autentici, pur presentando nella maggior parte dei casi, standard qualitativi inferiori in termini di *performance*, affidabilità o durata[39].

Il mercato della contraffazione si colloca all'interno di quell'area che viene comunemente definita «*grey market*» dell'economia globale, caratterizzata dalla mancanza di tracciabilità e da dinamiche elusive. Da qui la distinzione tra i c.d. *deceptive markets*, ossia mercati ingannevoli nei quali il consumatore, a causa della scarsa conoscenza del prodotto o a causa di informazioni fuorvianti, non è in grado di distinguere tra un prodotto autentico o falso; e i c.d. *non-deceptive markets* ove l'acquirente è pienamente consapevole della natura illecita o non originale del prodotto, optando deliberatamente per l'acquisto.

[39] A. M. Pinto da Cuncha Brandão - M. Gadekar, *The Counterfeit Market and the Luxury Goods*, in *Fashion Industry*, 2019, p. 1 ss.

La contraffazione *online* nel settore della moda si manifesta prevalentemente attraverso un doppio canale. In primo luogo, le piattaforme di *e-commerce* che consentono a venditori terzi di offrire direttamente prodotti ai consumatori (es. *Amazon*, *AliExpress*, *eBay*), trattandosi a volte di articoli con marchi identici o simili a quelli registrati, senza autorizzazione da parte del legittimo titolare[40]. Una dimensione ancora più complessa è riscontrabile nel contesto dei *social media*, ove le caratteristiche strutturali rendono particolarmente insidiosa l'individuazione degli autori delle violazioni. L'anonimato degli utenti, la brevità e la volatilità dei contenuti (si pensi ad esempio alle «*stories*» che hanno una durata effimera pari a ventiquattro ore o ai video in diretta), rendono il fenomeno particolarmente elusivo. L'intento è sempre il medesimo: sfruttamento parassitario della notorietà del marchio per ottenere un vantaggio economico e reputazionale diretto ovvero consistente in un aumento dell'*engagement* e visibilità, oltre alla raccolta fraudolenta di dati personali.

Nel *fashion system* digitale il confine tra imitazione lecita e contraffazione illecita risulta particolarmente sfumato. Alcuni studiosi discorrono di «*piracy paradox*»[41], una teoria secondo la quale il settore *fashion* prospera addirittura in funzione della facilità con cui i prodotti possono essere copiati, anche in modo sistematico. In tale prospettiva, la rapida diffusione delle imitazioni, inclusa quella facilitata dai canali online, non si tradurrebbe automaticamente in un danno per il mercato della moda nel suo complesso, ma piuttosto alimenterebbe un meccanismo di «obsolescenza indotta», in base al quale una copia stimola un ciclo continuo di innovazione e un ricambio di collezioni, nella prospettiva del c.d. dinamismo produttivo.

Nel quadro della lotta alla contraffazione online, merita di essere citata la sentenza della Corte di giustizia UE[42] ove la multinazionale

[40] Nonostante la predisposizione di linee guida interne e di meccanismi per contrastare tale fenomeno, il controllo preventivo risulta spesso essere insufficiente, privo di un monitoraggio costante e continuo, limitato a interventi che avvengono a seguito di segnalazioni.

[41] K. Raustiala - C. J. Sprigman, *The Piracy Paradox: Innovation and Intellectual Property in Fashion Design*, in *Virginia Law Review*, 2006, n. 92, p. 1687 ss.

[42] Corte giust. UE, 12 luglio 2011, causa C-324/09, *L'Oréal SA e altri v. eBay International AG e altri*.

francese *L'Orèal* accusa la piattaforma *eBay* di aver consentito la vendita non autorizzata, mediante il *marketplace*, di prodotti recanti il proprio marchio. La violazione si configurava nella commercializzazione di prodotti contraffatti, di campioni gratuiti non destinati alla vendita, nonché di prodotti privi di imballaggio originale. I giudici di Lussemburgo ritendendo che *eBay* rientri a pieno titolo nella categoria degli *Internet Service Provider* e che la sua attività, qualificabile come un vero e proprio servizio di assistenza nelle vendite, non può essere considerata meramente passiva e, dunque, non può essere soggetta all'esenzione di responsabilità prevista dalla Direttiva *e-commerce*[43].

Nel caso di specie *eBay* utilizzava il marchio *L'Orèal* a fini puramente promozionali, associandolo, tramite parole chiave, ad alcuni prodotti presenti sul proprio sito. La Corte, facendo tesoro di una precedente pronuncia, conclude che «per quanto attiene alla questione se l'uso della parola chiave corrispondente ad un marchio sia idoneo a recare pregiudizio ad una delle funzioni del marchio, (…) un pregiudizio del genere sussiste qualora l'annuncio non consenta, o consenta soltanto difficilmente, all'utente di Internet normalmente informato e ragionevolmente attento, di sapere se i prodotti o i servizi a cui l'annuncio si riferisce provengano dal titolare del marchio o da un'impresa economicamente collegata a quest'ultimo oppure, al contrario, da un terzo»[44]

Nell'ultimo ventennio, in concomitanza dell'espansione del commercio online e dell'importanza sempre più pregnante della presenza digitale per le imprese, soprattutto nel campo della moda, in cui il marchio rappresenta un *asset* intangibile di elevato valore, si è amplificata la rilevanza dell'*Internet Corporation for Assigned Names and Numbers*

[43] Nella sentenza della Corte giust. UE, 23 marzo 2010, causa C-236/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, viene individuata la responsabilità di un Internet Service Provider qualora «essendo venuto a conoscenza della natura illecita di tali dati, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi».

[44] Corte giust. UE, 8 luglio 2010, causa C-558/08, *Portakabin e Portakabin*. Per un commento dottrinale v. D. Danieli, *Piattaforme di e-commerce e contraffazione di marchi: cambi di paradigma nel regime di responsabilità regolato dal diritto dell'Unione europea?* in *Papers di diritto europeo*, 2023, n. 1, p. 23 ss.

(ICANN)[45], un'organizzazione internazionale no-profit istituita nel 1998 con l'obiettivo di coordinare e gestire il sistema globale dei nomi a dominio (*Domain Name System*) e dell'assegnazione degli indirizzi IP. Il suo ruolo fondamentale emerge nell'ambito della definizione delle regole e dei meccanismi attraverso i quali sono regolamentati i nomi a dominio che spesso rappresentano l'estensione digitale dei marchi. L'operatività dell'ICANN non consiste in un controllo preventivo inerente alla registrazione dei nomi a dominio, ma avviene *ex post*, mediante la gestione di eventuali dispute e attraverso l'implementazione di *policy* aggiornate in termini di prevenzione degli abusi.

Uno degli strumenti principali adottati da tale organizzazione per contrastare l'utilizzo abusivo dei *domain name* è la *Uniform Domain Name Dispute Resolution Policy* (UDRP)[46], una procedura di arbitrato internazionale per una risoluzione rapida, efficace e conveniente a tali tipologie di conflitti. L'operato dell'ICANN si integra con quello di altri organismi nazionali e internazionali che si occupano di proprietà intellettuale per un sistema armonizzato di protezione del marchio nel *digital environment*.

Un passo decisivo verso una regolamentazione più articolata e vincolante delle piattaforme digitali è avvenuto con l'emanazione del *Digital Services Act*[47], prova del vivace dibattito sociale e politico, non ancora sopito, sull'opportunità di un intervento normativo che possa armonizzare le discipline dei singoli Stati nazionali UE. Una sfida diffi-

[45] Cfr. H. Klein, *ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy,* in *The Information Society*, 2002, pp. 193-205.

[46] La procedura UDRP permette ai ricorrenti di richiedere una decisione extragiudiziale relativa al trasferimento o alla cancellazione di un dominio. Prima della sua introduzione non esisteva una regolamentazione uniforme per risolvere tali controversie. I titolari dei marchi si trovavano ad affrontare lunghi e costosi procedimenti legali per far valere i propri diritti.

[47] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 *relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE* (regolamento sui servizi digitali), entrato ufficialmente in vigore nel novembre 2022, obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri a decorrere dal 17 febbraio 2024, fatta salva la sua applicazione anticipata nei confronti dei fornitori di piattaforme *online* di dimensioni molto grandi e di motori di ricerca *online* di dimensioni molto grandi.

cile, in quanto la digitalizzazione è, per definizione, un terreno impervio. Il *Digital Services Act* prevede molteplici obblighi in capo ai *provider* allo scopo di contrastare la diffusione di contenuti illegali, garantire una maggiore concorrenza e sicurezza, rendere l'ambiente trasparente e sicuro, tutelare i diritti fondamentali e l'anonimato *online*[48]. Tale architettura poggia sui principi essenziali (che il nuovo regolamento fa salvi) della direttiva *e-commerce*; in particolare il principio dell'irresponsabilità del *provider* per i contenuti *user-generated* e il divieto di obblighi di sorveglianza e filtraggio preventivi.

La nuova disciplina europea mira a rafforzare la tutela preventiva e repressiva dei diritti della proprietà intellettuale, la cui disciplina impone una serie di obblighi di trasparenza, cooperazione e tracciabilità, in contrasto a fenomeni come la contraffazione, estremamente diffusa nella moda. L'obbligo di raccolta e conservazione delle informazioni sui venditori terzi, rappresenta un elemento chiave per identificare con più facilità i soggetti responsabili della commercializzazione dei prodotti illeciti, rendendo più efficace il sistema di *enforcement*.

L'approccio statunitense alla tutela del marchio online si è sviluppato invece attraverso *l'Anticybersquatting Consumer Protection Act* (ACPA), legge federale introdotta come emendamento al *Lanham Act*[49], con l'obiettivo di reprimere l'uso abusivo dei *domain name* cor-

[48] Cfr. G. M. Ruotolo, *Le proposte di disciplina di Digital Services e Digital Markets della Commissione del 15 dicembre 2020*, in *DPCE online*, 2020, 4; G. De Gregorio - O. Pollicino, *L'alba di nuove responsabilità sulle piattaforme digitali: il Digital Services Act,* in *AgendaDigitale.eu*, 15 dicembre 2020; F. Wilman, *The Digital Services Act (DSA): An Overview*, in *Nederlands tijdschrift voor Europees recht*, 2022, 9-10, p. 220, «[…] the DSA codifies the central criterion that, in order to be able to rely on the liability exemption, providers of hosting services should be neutral, in the sense that they do not play an active role of such a kind as to give them knowledge of, or control over, the information from users that they transmit or store. […] there is no reference to a requirement of passivity on the part of the service provider – its role may therefore be active to a certain extent, as long as it does not lead to knowledge or control […]. In this manner the DSA deviates somewhat from the e-Commerce Directive, which contained such a reference to passivity. It was that reference which, according to many, the CJEU wrongly applied also to hosting services».

[49] Definito «*an Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purpose*». United States Congress, *Lanham Act*, Pub. L. No. 79-489, 60 Stat. 427 (1946).

rispondenti a marchi registrati. L'ACPA è codificato nel 15 U.S.C. § 1125 (d) e consente ai titolari di marchi registrati di promuovere azioni civili nei confronti di chi registra o utilizza un nome a dominio identico o simile a un marchio registrato con «bad faith intent to profit from the mark», se dalla registrazione può derivare confusione nel pubblico o sfruttamento indebito della notorietà del marchio[50].

Negli Stati Uniti, così come altri Paesi di common law (es. Regno Unito, Canada), l'utilizzo del segno è alla base del sistema di tutela dei marchi; vige il principio del "*first to use*", che implica l'acquisizione della proprietà del marchio in capo a chi per primo lo abbia utilizzato. In altre parole, l'uso dimostrato del marchio potrebbe comportare di per sé l'acquisizione della titolarità del diritto, impedendo possibili registrazioni successive di marchi simili e pertanto in grado di generare confusione per il consumatore. Il diritto sul marchio sorge con l'uso effettivo nel commercio (*use in commerce*), anche in assenza di registrazione, atteso che quest'ultima natura facoltativa e non costitutiva.

Per converso, in Italia e nei paesi dell'Unione Europea il criterio più largamente adottato e applicato è quello del "*first to file*", in forza del quale il diritto spetta a chi per primo registra il marchio, seppure già utilizzato da altri. Il grande pregio di tale approccio è che rende più facile amministrare la gestione dei marchi e risolvere i contenziosi, avendo a disposizione un criterio oggettivo, cioè la data di registrazione, che può essere utile se non risolutiva nello sciogliere eventuali controversie.

Tale distinzione rileva dunque sul piano sostanziale, incidendo sulle modalità di acquisizione e di difesa dei marchi nei rispettivi ordinamenti. Si discorre di *common law trademarks* per indicare quei marchi non oggetto di registrazione formale, ma tutelati sulla base del principio del *first to use*. Tuttavia, i diritti che derivano dall'uso effettivo si estendono limitatamente all'area geografica in cui il marchio è stato concretamente utilizzato e riconosciuto dai consumatori. Ciò può comportare un indebolimento della posizione giuridica del titolare del marchio non

[50] A norma del 15 U.S. Code § 1063: «The term "use in commerce" means the bona fide use of a mark in the ordinary course of trade, and not made merely to reserve a right in a mark», ne consegue che è richiesto un uso in buona fede del marchio, reale e commerciale, e non meramente fittizio.

registrato, soprattutto qualora dovesse sorgere un conflitto con un soggetto che abbia registrato il medesimo marchio a livello federale ma che operi in un'area geografica differente. Attraverso lo studio comparato non è difficile scorgere il valore strategico della registrazione che, attribuendo una presunzione legale di titolarità sull'intero territorio nazionale, garantisce una tutela estesa e solida.

Seguendo la ricostruzione proposta, assume particolare rilievo la constatazione della presenza di un *fashion system* che ha profondamente integrato nel proprio funzionamento una delle caratteristiche culturalmente più significative del digitale, ovvero, la sua natura contaminata, trasversale e composita[51]. Orbene, la moda si intreccia sempre più con le diverse forme dei media e delle comunicazioni di massa, ove è preponderante la grafica, il design, la pubblicità. Pertanto, in un'epoca in cui l'identità di un *brand* può essere costruita o compromessa con un semplice clic, la protezione del marchio richiede non soltanto la predisposizione di strumenti giuridici adeguati, ma anche una profonda consapevolezza delle dinamiche digitali in continua evoluzione.

Quel che preme sottolineare è che, pur in presenza di delicate questioni giuridiche, le disposizioni contenute nei regolamenti europei rappresentano una solida base sulla quale costruire un nuovo quadro giuridico di riferimento e il *Digital Service Act*, grazie alla forza persuasiva delle sue norme, può senz'altro divenire un fattore trainante su scala globale, come del resto è dimostrato dall'ampio e vivace dibattito mondiale sviluppatosi intorno ad esso[52]. La prospettiva indicata sollecita una riflessione di più ampio respiro verso un sistema organico e armonizzato che ci consenta di stabilire quali siano, in concreto, i limiti applicativi degli strumenti digitali e le conseguenti responsabilità.

[51] Cfr. The *new frontiers of fashion law*, a cura di R.E. Cerchia - B. Pozzo, MDPI, 2021; E. Rosati - I. Calboli, *The Handbook of Fashion Law*, Oxford University Press, 2025; L. Palandri, *Digitalization and access to cultural heritage from the Italian perspective. A focus on digital archives and collections*, in *The Italian law of cultural heritage: A dialogue with the Unites States*, 2024, p. 123 ss.

[52] A. Turillazzi - M. Taddeo - L. Floridi - F. Casolari, *The Digital Services Act: an Analysis of its Ethical, Legal, and Social Implications*, in *Law, Innovation and Technology*, 2023, vol. 15, n. 1, p. 83 ss.; M. Husovec, *Priciples of the Digital Services Act*, Husovec, Martin. *Principles of the digital services act*, Oxford University Press, 2024.

REPRODUCTION, ARTIFICIAL WOMBS IN FRANCE AND U.S.: A NEW WAY OF BEING BORN

Veronica Caporrino

1. In the era of new procreative techniques, the study of the topic of genetic identity and parenthood, calls a methodological consideration. It must be carried out on an interdisciplinary basis that touches law, medical sciences[1], religion[2], etc. Assisted reproductive techniques are also of interest the social sciences: anthropology, psychology, sociology which traditionally they placed fertility, generativity and filiation with-

[1] The primary scientific and medical justification for these technologies is to save the lives and health of extremely preterm babies during wanted pregnancies. In thisi direction, see E.A. Partridge - M.G. Davey - M.A. Hornick - P.E. McGovern - A.Y. Mejaddam - J.D. Vrecenak - C. Mesas-Burgos - A. Olive - R.C. Caskey - T.R. Weiland - J. Han - A.J. Schupper - J.T. Connelly, *An extrauterine system to physiologically support the extreme premature lamb*, in *Nature Communications*, 2017, *https:// doi. org/ 10. 1038/ ncomm s15112*; H.M. Usuda - S. Watanabe - Y. Miura - M. Saito - G.C. Musk - J. Rittenschober-Bohm - H. Ikeda - S. Sato - T. Hanita - T. Matsuda, *Successful maintenance of key physiological parameters in preterm lambs treated with ex vivo uterine environment therapy for a period of 1 week*, in *American Journal of Obstetrics and Gynecology*, 2017, in *https:// doi. org/ 10. 1016/j. ajog. 2017. 05. 046.*

[2] The various connotations that religions ascribe to the body in same way recall creation. The body as a gift of Creation. Human is that body in which all creation becomes aware of its own mystery, its own existence. Human as consciousness of creation. The use of the spatial metaphor of "in/out" suggests that the state we are used to calling "consciousness" has a link to the condition of immersion. Depending on the case, the mind may be immersed in a task, encapsulated in an organ, device or cultural system, or it may simply be in a state of latency. Space and time in which we are immersed are transcendental. The condition that avoids this space-time localization is the divine one «He is the Place of the World, but the World is not His Place», Bereshit Rabbah 68, 9.

in kinship systems. Sociologists and scientists express doubts about the science of ectogenesis. A process in which an embryo grows independent of its mother's body. This technique, for some of them[3], is the logical evolution of neonatology, that allows premature babies to survive, or it is a technique that disconnect procreation from sexuality[4]. Assisted procreation techniques have opened up scenarios not only ethical, but also the legal one that need own regulation.

Also the religion is involved with the body, the incorporation. But what happens to all this inventory of corporeality, in the era of digitalization, that does not eliminate bodies but encodes them into disembodied, transferable patterns?

We would specified whose body is it; the person is a God creation[5], or is a creation of the nature, of a social power.

[3] R. Salam, *The End of Pregnancy: And the inevitable rise of the artificial womb,* 2014, in *http://www.slate.com/articles/news and-politics/culturebox/2014/10/ectogenesis theendof pregnancy.andthe-inevitable_rise_ofthe artificial.htmi.*

[4] J.B.S. Haladane, *Daedakus, or, Science and the future*, Cambridge University, 1923; H. Atlan, *L'uterus artificiel*, Points, 2005.

[5] According to Judaism, the human is seen as a being created in the image and likeness of God, composed of the spirit that lives inside the body, both in woman and man. Flesh, then, is a gift that God gives to people through creation, just like their spirit. The soul and body are considered a single entity that constitutes human's personality, so, the body is the material location of God's that define the state of purity and impurity of the faithful.

The Hindu tradition has developed a complex conception of the body, according to which humans are the result of a combination of material and spiritual elements: the material substrate that pervades all existence (prakriti) and the Supreme Being as eternal consciousness (Atman, the spiritual "Self," the spark of eternity in each being).

The Buddhist tradition has developed a complex system; here body and mind are a single human entity. Material form would consist of five provisional components called skandhas (form, feeling, perception, mental formations and consciousness). According to Christian tradition, the body is the place of spiritual knowledge, morality and hope in the Resurrection. In the Old Testament, there is no distinction between soul and body, between spirit and matter. The soul and the body are two complementary elements of which human is composed. Resurrection, according to the Christian faith, takes place through the body. Even in religious activities, the body plays an important role in various aspects of faithful. In baptism, or entry into Christian churches, it was and is administered through immersion of the body in water (although nowadays common forms include pouring water on the forehead). According to Islamic tradition, God created human from clay and

There are mythological antecedents to the contemporary idea of artificial wombs[6]. In ancient Egypt, the pregnant women turned to Isis, Goddess of Fertility and Motherhood and keeper of powerful magic[7]. The birth was an Act of the Gods[8].

Medical technologies and new discoveries, however, gradually separated out any magical aspects attributed to the feminine. The myth of ectogenesis was born recently. The invention is attributed to the British scientist and professor John B. S. Haldane in the 20th century[9].

In carrying out this study we believe it is appropriate to start from the analysis of the transformations of the social reality in which legal regulation lives. This situation gives rise to a series of legal issues concerning multiplication of the figures at the birth scene, post-mortem fertilization, destiny and the use of cryofrozen embryos. The limits within which one can intervene on the genetic heritage of the unborn child, transplant of uterus and ectogenesis (whose child is whose when gestation occurred in a artificial uterus).

Assisted reproductive techniques, separating conception from sexuality, where they move conception outside the bodies of masculine and feminine. They redefine the intended meaning that men and women attribute to sexuality and the sexual body. The objective is not to attest to the influence of so-

breathed the spirit of life into him. Every body has a conscience, as the inviolable space in which the value and dignity is enclosed and, therefore, as a source of morality. There are circumstances (vegetative states), life forms (what exactly does it feel like to be a bat?), ethical dilemmas (is there a time when it is appropriate to "pull the plug?"), which can make people to wonder if there is or has been "someone" in there.

[6] One recalls, the myths associated with the Indian Mahabharata that tell the story of Queen Gandhara, who, out of jealousy, caused her sister-in-law, Kunthi, to miscarriage. Kunthi planted one hundred pieces of her shattered fetus in one hundred jars of ghee, and these became the one hundred princes Kaurava. The conception was opalescent and enigmatic phenomenon veiled by feminine mystery and divine intervention. J. Hughes, *Artificial Womb: a short history*, in *Orbis Idearum*, 9, 2021, p.13 ss.

[7] *Ibidem.*

[8] G. Chamberlain, *Historical perspectives on health, Childbirth in Ancient Egypt*, in *The Journal of the Royal Soc'y for the promotion of health*, 2004, p. 284.

[9] The Professor Haldane, in a 1923, in a conference *Daedalus, or Science of the Future,* in which he imagined a student in the year 2070 talking about the landmark discoveries of the two last centuries. So, J.B.S. Haldane, *Daedalus, or, science and the future*, cit.

cial transformations on legal norms, but rather to understand whether legal norms are able to contain and support evolution. Whether they guarantee the necessary protection also for new and unprecedented needs or, instead, whether they are subject to tensions or interpretative twists.

2. Aldous Huxley in his book *The New World*, written in 1932, discusses a new concept named *Ectolife Artificial Womb Facility* that is, the realization of the artificial human. In this book, the new society is based on the principles of mass production applied in Ford's automotive industries to the production of the *Model T*. Ford. Mass production is also applied to human reproduction, made completely extrauterine. Human embryos are produced and allowed to develop in special factories according to pre-established quotas planned by national governors. The French biologist Henri Atlan in 2005, in the book *L'Uterus Artficiel* attempted to analyze the consequences of introducing artificial wombs into the reproductive technology market. According to philosopher Sloterdijk[10], during gestation, blood sharing, suspension in the amnion and acoustic communication with the outside world occur within an immersive media environment defined as a microsphere. Recovering Sloterdijk's thought, we discuss *cyborghood*, a mode of hybrid embodiment influenced by technological, cultural and physiological factors.

The theme concerns science fiction and ideological notations, hypothesizing a symbiosis between human and machine in the synthesis of a *cyborg*. The perspective of post-humanism, which seems to imply, rightly or wrongly, a future in a which human will come to be what he desires. The human is crossed by the temptation to be immortal alone, without God, without a God. It is the transhumanist temptation, which sees in the graft between human and machine, the frontier of the new humanity, a technical promise of possible immortality. An attitude seems to be emerging that tends to overcome the inevitability of death, imposed by the human condition.

The human beyond the human. Transhumanism is a scientific-technological researcher that aims to overcome all human limitations through technology. The aim is to redefine the notion of human nature.

[10] P. Sloterdijk, *Spheres Volume I: Bubbles (Microspherology)*, Semiotext, 1998.

There is a belief that humans can be transformed through technosciences with a condition located beyond human and represented by the symbol H+. The human reality is seen as a moment of transition, within a new evolutionary phase, aimed toward a post-human future.

New technologies are grafted onto living bodies, redrawing unexpected boundaries. The techo-assembled figurations and souls, like scifi grafts, are models of a crasis on the border between human and non-human that guide us toward a depiction of the hybrid. These representations touch the limits of the norm, they revive an idea of Golem, the artificial hybrid human. It is what is known as uncanny. The techno-hybrid figurations show the gray and uncanny zone of the possible, of the in-potentia, and offer the view of some feared scenarios.

In the transhuman era, law should undergo similar metamorphoses. For example, transhumanism could influence general principles of law, such as, the principle of equality.

In the transhuman immortal context, some authors go as far as to identify new rights, among these the right to cognitive freedom; the right to mental privacy; the right to mental integrity; and the right to psychological continuity[11].

Ectogenesis involves the implantation and full development of the fetus outside the human body, by *in vitro* fertilization and in an artificial womb[12].

[11] For example, Chile approved a law the protection of neurorights into Costitution. Faced with the progress of technology and the emergence of new rights related to it, every State must intervene to ensure the protection of people. With this rule, Chile qualifies mental identity for the first time in history as a right that cannot be manipulated.

[12] The first known incubator for preterm infants was developed in France in 1880 when obstetrician Etienne Tarnier placed infants in a wooden box with a hot water bottle. Incubators for infants were subsequently exhibited at fairs in Germany, the United States, and Great Britain to much acclaim, and probably contributed to stimulating Haldane's imagination in 1923. But it was not until after World War Two that special hospital units for newborns were first built in Britain and the United States. See, A. Ferreira, *The Fantasy of Ectogenesis in Interwar Britain: Texts and Contexts*, in *Exchanges between Literature and Science from the 1800s to the 2000s: Converging Realms*, Cambridge, 2017, p. 134 ss. In the 1960s, specialized incubators with controlled oxygen and temperature were introduced. By the 1970s, births starting at 24 weeks were treated in neonatal intensive care units. So, A. Prasad, *How Artificial Wombs Will Change Gender, Family and Equality*, in *The Guardian*, 2017.

The artificial wombs is a technological device that allows gestation in place of the woman's uterus in an extracorporeal gestation, imitating the structure of a natural uterus. The use of artificial wombs is linked to the issue of surrogacy. The permissive solution is found not only in legal contexts different from the Italian[13] one (such as America, Asia,

[13] See l. n. 40/2004. In particular, the art. 12, par. 6, prohibits «the marketing of gametes or embryos or surrogacy»13, while art. 5 reserved only for married adult couples of different sexes and cohabitants, the use of heterologous fertilization. For the criminal aspects of the case, see T. Trinchera, *Limiti spaziali all'applicazione della legge penale italiana e maternità surrogata all'estero*, in *Riv. it. dir. proc. pen*., 4, 2017, p. 1391 ss.; V. Scalisi, *Maternità surrogata: come "far cose con regole"*, in *Riv. dir. civ*., 2017, p. 1097 ss. U. Salanitro, *Norme in materia di procreazione medicalmente assistita*, Sub *artt. 1-3*, in *Comm. c.c.*, Utet, 2010, p. 1657 ss. The author say that: «a differenza di quanto comunemente rappresentato, non è vero che il nostro Paese prima del 2004 era afflitto da una sorta di Far West procreativo. Piuttosto, l'accesso alle tecniche di procreazione assistita era disciplinato da circolari ministeriali e sottoposto al codice deontologico medico allora vigente le cui regole, pur sottoposte a torsioni interpretative, erano tendenzialmente rispettate». F. Ruscello, *La nuova legge sulla procreazione medicalmente assistita*, in *Fam. dir*., 2004, p. 628 ss. nevertheless the art. 9, l. n. 40/2004, establishes that «In caso di applicazione di tecniche di tipo eterologo in violazione del divieto di cui all'articolo 4, comma 3, il donatore di gameti non acquisisce alcuna relazione giuridica parentale con il nato e non può far valere nei suoi confronti alcun diritto né essere titolare di obblighi». In case of application of techniques heterologous type, those who donate the gametes do not acquire any relationship legal parental rights with the born child and cannot assert any rights against him right nor be the holder of obligations. However, this impediment is now superseded by living law, through restrictive application of the regulatory data, limited to cases in which the donor is "external" with respect to the family project. See App., Perugia 22 agosto 2018, in *De Jure*; Trib. Pisa, 20 dicembre 2017, in *Ilfamiliarista.it*, 27 marzo 2018; Cass., 30 settembre 2016, n. 19599, where it is stated that «parlare di maternità surrogata nel caso in cui una donna doni i propri ovuli ad un'altra donna affinché questa possa concepire un figlio proprio; la surrogazione di maternità, infatti, si caratterizza per l'esistenza di una donna terza rispetto al rapporto di coppia, che mette a disposizione la sua capacità riproduttiva». App. Bari, 13 febbraio 2009, in *Giur. merito*, 2010, 2, p. 349; M. Dell'Utri, *Maternità surrogata, dignità della persona e filiazione*, «in tema di maternità surrogata, il solo fatto che la legislazione italiana vieti l'applicazione di detta tecnica, non è di per sé un indice di contrarietà all'ordine pubblico internazionale, a fronte di legislazioni (come quella inglese e quella greca) che prevedono una disciplina sostanzialmente differente e conseguentemente va accolta la domanda di riconoscimento nello Stato italiano dei provvedimenti giurisdizionali britannici che riconoscono lo stato di genitorialità a soggetti che abbiano utilizzato suddetta tecnica».

Oceania and some South African states[14]) but also in Europe (such as United Kingdom[15], Greece[16], Portugal[17], Ciprus[18] and athers). The France[19], German[20], Spanish[21], Austrian[22], Switzerland[23] Danish[24] and Norwegian[25] legal systems follow the Italian one.

This study offers a comparative analysis of the prospective legal impact of the use of artificial wombs in the United States and France. The choice of these systems is dictated by the fact that while the United States presents an open approach to the use of artificial wombs, France

[14] G. Sciancalepore, *La maternità surrogata. Profili comparatistici*, in *Comparazione e diritto civile*, 2021, p. 445 ss.; M. Di Donato, *Divieto di maternità surrogata e ordine pubblico internazionale: profili comparatistici*, in *Annuario dir. comp.*, 2022, p. 367 ss.; T. Bortolu, *La gestazione per altri tra diritto alla procreazione, dignità umana e superiore interesse del minore. Una riflessione comparatistica*, in *Actualidad Jurídica Iberoamericana*, 2022, p. 458 ss. S. Aceto di Capriglia, *I profili critici etico-giuridici concernenti la maternità surrogata. Un confronto tra modelli*, in *Corti salernitane*, 2019, p. 3 ss.; Id., *An Anthropological Reading of Surrogacy and the Role of Supreme Courts*, in *The Italian Law Journal*, 2020, p. 319 ss.; A. Stazi, *Genomica umana e maternità surrogata nel diritto comparato: pluralismo giuridico e dinamica dei modelli*, in *Comparazione e diritto civile*, 2019, p. 881 ss.

[15] See *Surrogacy Arrangements Act*, 1985.

[16] See, l. n. 3089/2002 and l. n. 3305/2005, as integrated by l. n. 4272/2014, which allowed access to surrogacy also to foreigners, as long as they were residents in Greece. The law n. 4958/2022 raised the mother's age limit intentional to access the practice, which was thus changed from 50 to 54 years.

[17] See l. n. 90/2021. For the doctrine see L. Bozzi, *La legge portoghese in tema di gestazione per altri. Riflessioni e interrogativi (su questa e su ogni legge in materia)*, in *Eur. dir. priv.*, 2024, p. 299 ss.

[18] See l. n. 69/2015.

[19] Loi no 94-653 du 29 juillet 1994 *relative au respect du corps humain*, in *https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000549619.*

[20] See art. 1, *Embryonenschutzgesetz*,13 Dezember 1990 (BGBl. I S. 2746); *Embryo Protection Act* of 13 December 1990, last amended by Article 1 of the Act of 21 November 2011, in *https://www.gesetze-im-internet.de/eschg/BJNR027460990. html.*

[21] See art. 10 *ley* n. 14/2006; see also art. 32 *ley* n. 1/2023.

[22] *Fortpflanzungsmedizingesetz - FmedG* e *Bundesgesets mit dem Regelungen über die medizinich Fortpflanzung*.

[23] *Bundesgesetz über die medizinisch unterstützte Fortpflanzung* (*Fortpflanzungsmedizingesetz, FMedG*), 18 December 1998.

[24] See art. 31 law n. 1097/2014.

[25] See art. 2 *Children and Parents Act*, 1981 and artt. 2-15 *Medical Humane Use and Biotechnology* Act, 2003.

follows an open approach inspired, however, by prudence. Both these systems have addressed the issue of artificial wombs[26], in particular, the status of the ectogenetic embryo, the concept of parenthood and access to ectogenetic technology. It traces the differences in how the technology may be implemented in a jurisdiction where reproductive technology is highly regulated (France)[27] and one where it is relatively unregulated (United States)[28].

The semi-open attitude followed by France differentiates it from other European states that still have rigid closures towards these techniques. The comparison between an open system and a closed one with some openings allows us to make legal assessments in terms of protections in order also to verify the possibility of transplanting the French solution into other European systems.

3. France constitutes an interesting case study for investigating reproductive policy technologies. Historically, France has supported pronatalism and the policy aimed at increasing the size of the population, through the classic family model and repressive laws on contraception and abortion[29]. France established its first commercial sperm banks in the early 1970s, in public hospitals with minimal oversight. Only later

[26] In the italian system the mechanism that releases procreation from pregnancy and childbirth is described as capable of overthrowing the relations between the two sexes and to offend the dignity of procreation. So, C. Bulletti - C. Flamigni, *Fare figli. Storia della genitorialità dagli antichi miti all'utero artificiale*, Edizioni Pedragon, 2017, p. 210.

[27] S. Reineke, *New Reproductive and Genetic Technologies and Women's Rights in Contemporary France*, in *International Journal of Feminist Approaches to Bioethics*, 2008, p. 91 ss. Loi no. 94-653 du 29 juillet 1994, cit. Loi no. 94-654 du 29 juillet 1994 *relative au don et a Tutilisation des elements et produits du corps humain, a l'assistance medicale a la procreation et au diagnostic prenatal*; Loi no. 94-630 du 25 juillet 1994 *modifiant le livre II bis du code de la sante publique relatif a la procreation des personnes qui se pretent a des recherches biomedicales*, in *http://www.Legifrance.gouv.fr.*

[28] On the lack of federal government regulation relating to reproductive technologies, see K. Riggan, *Regulation (or lack thereof) of assisted reproductive technologies in the* U.S. *and* abroad, 4, 2011, in *https://cbhd.org/content/regulation-orlack-thereof-assisted-reproductive-technologies-us-and-abroad.*

[29] In this direction, we recall, Simon Veil as synonymous with the law she drafted that legalised abortion in 1975, that became a landmark of feminism and secularism. G. Allwood, K. Wadia, *Women and politics in France 1958-2000*, Khursheed Wadia, 2000.

professionals start pressing for a stronger legal framework. Their demands became more insistent in the 1980s. The French government created in 1988 the *Commission Nationale de Mèdecine et de Biologie de Reproduction* to licence private and public clinics for trials on assisted conception. In 1992 it took on the additional responsibility of prenatal genetic screening. Through the benefits of reproduction the first French *test tube baby* was done in 1982, but the French legislator strictly limits its use. In reference to assisted reproduction, the *Public Health Code* establishes that this technology will be used only to remedy diagnosed pathological infertility or to avoid transmitting a very serious disease to your unborn child or to another member of the couple.

France accepts the assistive reproductive technologies but strongly resists the reproductive technologies[30]. In fact, the Court of Cassation has considered surrogacy an act against the French fundamental principle of «non-commercialisation du corps humain»[31]. The legislator followed the Court's decision by inserting in the *civil code* a provision that specifically states «toute convention portant sur la procréation ou la gestation pour le compte d'autrui est nulle»[32].

The use of assisted reproductive technologies demonstrates the tension between the conservative and restrictive legislative push on assisted reproductive technologies. France occupies an intermediate position in this filed; it accepts assisted reproductive techniques but is opposed to more innovative reproductive technologies. The French attitude towards surrogacy is much less vague than towards *in vitro* fertilization. *Mater semper certa est*. Based on this maxim, French law established its principles regarding filiation. Also the jurisprudence says that the principle under French law is that «la mère de l›enfant est celle qui accouche»[33]. «La maternité peut être contestée en rapportant la preuve que la mère n'a pas accouché de l'enfant» (article 332 civil code). Re-

[30] J. A. Robertson, *Reproductive Technology in Germany and the United States: An Essay in Comparative Law and* Bioethics, in *Columbian Journal of Transnational law*, 2004, p. 189 ss.

[31] Court of Cassation Ass. plén., May 31, 1991, no. 90-20.105.

[32] Civil Code, art. 16-7.

[33] Court of Cassation, Apr. 6, 2011, no. 72.

garding children born through surrogacy abroad, it is interesting to note that the European Court of Human Rights has condemned France for failing to recognize the relationship between a father and his biological children born as a result of surrogacy arrangements abroad. The Court in *Mennesson v. France and Labassee v. France* states that, in the absence of uniform European legislation, even if it is necessary to leave a wide margin for the appreciation of the States, the same must be limited when the kinship or relationship involves a fundamental aspect relating to the identity of the subjects[34]. The *gestation pour autrui* is explicitly prohibited pursuant to articles 16-7 and 16-9 of the civil code and articles 227-12 and 227-13 of the penal code, as it is considered contrary to French national and international public order.

After several years, the *Court of Cassation* has recognized the legal motherhood of Mrs. Mennesson, intended mother of twin girls, born in California through surrogacy[35]. This historical turning point, which follows the advisory opinion of the European Court of Human Rights, favors the minor's right to recognition of the filial relationship (article 8 European Convention on Human Rights) over the prohibition. The decision closed a long legal battle. It ruled that the refusal to recognize the filial relationship exceeded the State's margin of appreciation, violating the right to private and family life.

A woman might use an egg donor, so she might be the legal mother of the child to whom she gave birth. However, the woman who seeks surrogacy will not be recognized as the legal mother of the child even if

[34] According to the Court, in this situation, the right to respect for the private life of minors had been significantly violated, preventing the recognition and establishment of legal relationships between minors and their parents and both France and Italy (*Paradiso e Campanelli c. Italia*, 27 January2015) had exceeded the permitted margin of appreciation by violating it the art. 8 ECHR. The protection of the best interests of the minor justifies, according to the Court, also the illegitimacy of a possible national decision to remove the minor from his parents customers and pave the way for adoption. The declaration of adoptability and foster care of the minor in a new family must be extreme solutions to be adopted with the character of residuality, since the protection of the minor's interests over one's own interests must be paramount parental relationship now formed, biological or otherwise.

[35] Court of Cassation, Arrêt n. 648, 4 Octobre 2019. See, recently European Court of Human Rights, 22 november 2022, nn. 58817/15 e 58252/15, *D.B et a.* v. *Swiss.*

the child has been conceived with her own egg[36]. This approach is in line with French law's refusal to recognize the legal effects of surrogacy agreements concluded abroad[37]. The approach introduces unequal treatment between women and men which genetics and biology are entangled with regards to procreation. The genetic father can be the father of a child conceived through surrogacy abroad who will be recognized as the child's legal father in France. This inequality will be exacerbated by the use of artificial wombs. Perhaps it might be easier for the biological father to be recognized as legal parent of the ectogenetic child compared to the non-gestational mother. The artificial womb creates a new legal issue: the child whose gestation would have occurred entirely in an incubator will technically be born to a "machines". Artificial wombs could be among in the provisions of Title IV of the Public Administration Code[38], which regulates assisted persons reproductive technologies in general, unless artificial wombs are regarded as such an invasive technology that it would represent more than a mere assistance to human reproduction.

4. The United States is missing one federal regulation of reproductive technologies[39]. At the state level, medical activity is regulated, with reference to medical treatments for infertility, through the issuing of licenses to professionals. Reproductive use of technology is also left to the self-regulation of the medical profession[40].

In general, the U.S. is a highly permissive country towards the assistive reproductive technologies. If we would compare the European

[36] Court of Cassation, 17 December 2008, no. 289. The Court says that «where the national court gave right to the French authorities that refused to enter the birth certificates resulting from a surrogacy agreement in the French register of births».

[37] European Court of Human Rights, 26 Juin 2014, no. 65192/11, Mennesson c. Francia. The European Court of Human Rights totally prohibiting the establishment of a relationship between a father and his biological children born following surrogacy arrangements abroad was in breach of the Convention.

[38] Code de la Santé Publique, Title IV – *Assistance mèdicale à la procreation* and *Mèdical Reproductive Assistance.*

[39] So, K. Riggan, *Regulation (or lack thereof) of assisted reproductive technologies in the U.S. and* abroad, 2011, cit.

[40] J.A. Robertson, *Reproductive Technology in Germany and the United States: An Essay in Comparative Law and Bioethics*, cit., p. 191.

and U.S. approaches on reproductive technology, we must note that the reception of assistive reproductive technologies in the U. S. cannot be adequately understood without an appreciation of the country's long tradition of individual freedom, free markets and free enterprise guidance and granting broad autonomy to doctors and others professionals[41].

The regulation of embryos for *in vitro* fertilization developed in the U. S. in response to deep political divides over abortion. Scientists, startups, women and patient groups who advocated for improved competitiveness, broader reproductive rights, privacy for individuals, and better access to therapeutic innovations.

The status of *in vitro* fertilization embryos remained ontologically, morally and administratively ambiguous. In the absence of uniform regulation, a large, poorly regulated market has developed. A market indifferent to the moral status of surplus embryos obtained through in vitro fertilization created to satisfy consumer demand.

The lack of a solution resulted in a regulatory patchwork that delegated the governance of these entities to state agencies, professional associations, and the market.

Also the laws on surrogacy vary from state to state[42]. Some states, like Louisiana, for example, have issued statutes declaring surrogacy contracts void and unenforceable, others, like New York, even penalize the parties to a subrogation contract, some, like Washington, distinguish between paid and unpaid surrogacy; and still, some states, like Florida, allow but regulate surrogacy, and some states, like Colorado, are simply silent on the issue.

The *Born-Alive Infants Protection Act* of 2002 protects the rights of any live-born infant at any point in development[43], including those who survive abortion attempts. However, it is unclear whether the pro-

[41] *Supra* note 37.

[42] *Guide to State Surrogacy Laws*, 2007, in *https://www.americanprogress.org/issues/women/news/2007/12/1 7/3758/guide-to-state-surrogacy-laws/.*

[43] E.C. Romanis, *Challenging the "Born Alive" Threshold: Fetal Surgery, Artificial Wombs, and the Limits of Legal Personhood*, in *Medical Law Review*, 2020, p. 93.

cess of artificially extracting a fetus and placing it in an artificial womb constitutes a "birth" under the statute's legal definition.

The artificial womb challenges the foundations of legal parenthood. In the current system, both parental rights and duties are established based on two important aspects of the relationship between an individual and their child. The biological bond and the gestational bond with the child. In surrogacy cases, courts have focused on intent, as established by the California Supreme Court in *Johnson v. Calvert*. The Court held that the intended parents, not the gestational surrogate, are the legal parents.

In the U. S. definitions of personhood have long been anchored at birth, the point at which an individual is granted full legal status and protection under the Constitution[44]. The study on artificial wombs cannot ignore the issue of abortion. The possibility for the embryo to survive outside the woman's body, while relying on another type of host, the ectogenetic incubator implies profound changes, in ways in which abortion is regulated.

In the case *Roe v. Wade*[45], the Supreme Court of the U. S. recognized the constitutional right to have on abortion. In the subsequent case *Planned Parenthood v. Casey*[46], the Court ruled that the right to abortion is an extension of women's right to privacy. This principle seemed threatened by the introduction of the artificial womb.

The U.S. Supreme Court overruled the constitutional right to abortion on June 24, 2022, in the case of *Dobbs v. Jackson Women's Health Organization*, since the right to abortion is no longer a right protected by the Constitution. Although *Dobbs* removed abortion protections, it did not eliminate individuals' liberty rights under the *Due Process Clause*. Requiring fetal transfer rather than termination may violate bodily autonomy and an individual's right to refuse medical treatment. A critical

[44] A. Crocker, *Are We Legally Ready for Artificial Wombs?*, in *Find Law*, 2019.

[45] *Roe v. Wade*, 410 U.S. 113, 164, 1973. On June 24, 2022, the Supreme Court overruled *Roe v. Wade* with the *Dobbs v. Jackson Women's Health Organization*, eliminating the federal constitutional right to abortion. The right to terminate a pregnancy is not protected by the Constitution, giving individual states the power to regulate or ban the procedure.

[46] *Planned Parenthood v. Casey*, 505 U.S. 833, 1992.

legal question arises regarding the appropriateness of protecting fetuses implanted in an artificial womb, particularly the protection of personality rights before birth. The Supreme Court's decision in *Gonzales v. Carhart*[47], which upheld the constitutionality of bans on certain abortion methods once the fetus reaches viability, takes on a different meaning when read through the lens of the use of artificial wombs.

In a post-*Dobbs* society, where federal abortion rights have been dismantled, the use of artificial wombs risks increasingly undermining the constitutional understanding of bodily autonomy and reproductive freedom[48]. States could attempt to rationalize new restrictions on abortion by favoring the use of artificial wombs based on the possibility that they offer a non-lethal alternative, thus shifting the focus away from maternal weight.

There is pressure on the question of whether the right to abortion is «the right not to be pregnant» or «the right not to procreate»[49]. The distinction is only theoretical. The science of ectogenesis believes that a fetus can be removed from a woman's womb and be immediately re-implanted into a artificial womb, escaping the *death* of an abortion[50]. We can glimpse in the Supreme Court's decision the desire to fully protect life by also admitting artificial gestation, decreeing the death of abortion. In an extreme scenario, governments could require the extraction of the fetus and the artificial gestation of the fetus under the guise of protecting life.

5. In order to draw some considerations we can say that the similarities between ectogenetic incubators and existing surrogacy agreements justify the common application of some broad principles. First, ectogenetic incubators can be an alternative for surrogacy. The promise of artificial wombs could have considerable advantages over classic surrogacy.

[47] *Gonzales v. Carhart*, 550 U.S. 124, 2007.

[48] J.E. Brown, *How Viable is Viability? Artifi cial Womb Technology and the Threat to Abortion Access*, in *Michigan Journal Gender Law*, 2024, p. 31.

[49] C. Kaczor, *The ethics of abortion, women's rights, human life, and the question of justice*, Taylor and Francis, 2015.

[50] A. Alghrani in *The Legal and Ethical Ramifications of* Ectogenesis, in *Asian Journal WTO & International Health*, 2007, p. 187.

Like the *in vitro* fertilization, ectogenetic technology has the potential to overcome a natural inequality between fertile couples and infertile couples. One difference: the *in vitro* fertilization focuses primarily on fertilization, ectogenetic technology focuses on *both* the gestation period and fertilization.

The use of ectogenetic incubators would suppress any concern regarding the gestational carrier's subsequent withdrawal of consent or willingness to pursue the pregnancy when the intended parents want it terminated. Some authors argue that artificial wombs will bring about a new. It was in the social liberation of women, «freeing them from tyranny of their reproductive biology»[51].

Access to *in vitro* fertilization in French law is limited both in terms of who can access it and for what purposes. Only heterosexual couples, alive and of reproductive age, have access to reproductive assistance. The access to assisted reproductive technologies is aimed at remedying just the diagnosed pathological infertility or to avoid of a serious illness to an unborn child; in others words means that the difficulty conceiving a child or early menopause does not guarantee the couple access to *in vitro* fertilization. In the United States, regulation of assisted reproduction is patchy; in particular, the private market (doctors, health facilities) manages the service; this means that it grants the possibility to use such techniques at its own discretion although it is still subject to the general rules of torts and contracts[52].

There is a doubt: if the environment surrounding fertilization and the first cell divisions can influence the development of the fetus. Raising a child in a «plastic box» can affect his emotional and social development. We wonders what kind of child one produces from a liquid medium inside a plastic box[53]. The use of artificial womb could pose a risk: women they may increasingly have the *duty* to give up reproduc-

[51] A. Pinteric, *Ectogenesis as a Theme in The Dialectic of Sex: The Case for Feminist Revolution*, 2025, in *https://embryo.asu.edu/pages/ectogenesis-theme-dialectic-sex-case-feminist-revolution-1970-shulamith-firestone*.

[52] About these differences, see C. Rosen, *Why Not Artificial Wombs?,* in *New Atlantis*, 2003, p. 67.

[53] J. Rifkin, *The end of pregnancy*, in *The Guardian*, 2002, also in *http://www.theguardian.com/world/2002/jan/17/gender.medicalscience*.

tion sexuality and pregnancy[54]. However, it could also have some advantages: interventions of genome editing may be easier if the embryo develops not in a human body, but in a mechanical device.

The possibility to intervene on the genetic heritage of the embryo at the time of conception or during its development raises moral and legal issues. Do the aspiring parents have the right to stop his development? Or do they not have this right because the embryo is viable?[55]

To try to give an answer we start from the right to evacuation and the right to termination. Ectogenetic gestation separates the right to evacuation (the right not to be pregnant) from the right to termination (the right not to procreate). With artificial wombs, the fetus can be extracted from the woman's body and transferred to an incubator, allowing the gestation to continue without the mother's physical involvement. This could limit the woman's right to decide the fate of the fetus, as her physical integrity would no longer be directly involved.

The concept of viability (the ability of the fetus to survive outside the mother's body) is central to abortion rights. Especially in the U.S., with artificial wombs, viability could technically be achieved immediately after fertilization, making it more difficult for women to exercise the right to terminate the gestation.

Regulating the right to terminate ectogenetic gestation will require balancing parental rights, fetal protection, and ethical considerations. French and U.S. legislators will need to address these challenges with new laws and legal definitions[56].

6. Under US and French law, human embryos occupy a provisional category, being considered more than just human tissue, but less than real people[57].

[54] S. Kennedy, *Ectogenesis and the value of gestational ties*, in *Bioethics*, 2024, p. 7.

[55] R. Tong, *Out of Body Gestation: In Whose Best Interests*, in *Ectogenesis. Artificial Womb Technology and the Future of Human Reproduction*, eds. S. Gelfand, J.R. Shook, John R. Shook, 2006, p. 59 ss.

[56] J.H. Schultz, *Development of E elopment of Ectogenesis: How Will Ar ogenesis: How Will Artificial W tificial Wombs Aff ombs Affect the Legal Status of a Fetus or Embryo?*, in *Chicago-Kent Law Review*, 2009, p. 877 ss.

[57] So, D.K. Katz, *The Legal Status of the Ex Uteri Embryo: Implications for Adoption Law*, in *Capital University Law Review*, 2006, p. 303 ss.

Based on this assumption, the comparison between the French and American systems allows us to make some reflections. If the artificial wombs, in French law, can fall within the current provisions of Title IV of the Public Administration Code which generally regulate the reproductive technologies of assisted persons, unless the artificial uterus is considered such an invasive technology as to represent something more than simple assistance to human reproduction, it can be admitted that, as in the US law, the use of the artificial uterus technique could represent a new way of giving birth to a new body.

A new "way of being born" which in the US legal system, characterized by an open approach followed by the legislator, is also confirmed in jurisprudence. In particular, on the question of whether parents have the right to arrest development, it suggests applying the provisions on frozen gametes to ectogenetic fetuses, even if frozen embryos, compared to ectogenetic fetuses, are already implanted, growing and engaged in the process of realizing a parental plan[58]. If equalization is possible, then respect for fetal life in the early stages of gestation requires the adoption of rules that limit the arbitrary decisions of parents regarding the fate of the fetus[59]. This solution, although surrounded by regulatory fragilities and as such not yet verified, could also be adopted by the French legislator. Recently, in addressing the problem of the declining birth rate, he envisaged the establishment of thirty centers for the freezing of gametes and the free service. This prudent opening would lead to a semi-convergence of models, at least in terms of parental responsibility regarding the future of the fetus[60].

Still. Before allowing the use of artificial wombs, legislators should establish the time limit from which reversal is possible, i.e. whether the couple's consent to continue the pregnancy until delivery is irrevocable once the embryo has been successfully inserted into the artificial womb. The technological box that allows the fetus to develop affects the development of the personality from the inside. The legislative concern should be to guarantee, in the face of new procreative techniques,

[58] *Davis v. Davis,* 842 S.W.2d 588, 1992.

[59] A. Alghrani in *The Legal and Ethical Ramifications of Ectogenesis*, cit., p. 203.

[60] A. Crocker, *Are We Legally Ready for Artificial Wombs?*, in *Find Law*, 2019.

compliance with the conditions considered best for the development of the personality of the newborn[61]. The use of an artificial womb also raises questions of liability. If a "womb" malfunctions or fails, causing injury or death, is this medical malpractice, technological malpractice, or wrongful death? Unlike traditional pregnancy, where individual biological factors can influence the success or failure of the pregnancy, in this case full responsibility is placed on doctors and biotechnology developers. Artificial gestation may also require new categories of responsibilities.

The concepts are further complicated by intentional harm, whether caused by a professional, a third party or a system developer.

Legislative and jurisprudential openings that meet the "desire" to have a child must find a balance between rights. Is it possible to arrive at the recognition of a "right" to create it in the laboratory, being able (perhaps) in the future to also choose sex, hair color or other physiognomic characteristics or even a "right" to purchase it, determining its most abject reification, so as to be "born by contract"?[62] The law is called upon to make its contribution to suggest proposals (now undeferrable) which are inspired by the canons of proportionality and reasonableness, in the context of parenting which oscillates between legitimacy, truth and responsibility[63].

The realization of ectogenesis eliminates the necessary presence of a body. The body becomes superfluous, indeed it disappears[64]. «L'ecto-

[61] Italian Constitutional Court, 18 june 2019, n. 221.

[62] F.D. Busnelli, *Nascere per contratto?*, in *Rass. dir. civ.*, 2004, p. 43 ss. Topics that intercept the delicate problem of cloning human. Hans Jonas, according to whom cloning is « nel metodo la piú dispotica e nel fine allo stesso tempo la piú schiavistica forma di manipolazione genetica; il suo obiettivo non è una modificazione arbitraria della sostanza ereditaria ma proprio la sua altrettanto arbitraria *fissazione* in contrasto con la strategia dominante nella natura». H. Jonas, *Cloniamo un uomo: dall'eugenetica all'ingegneria genetica*, in Id., *Tecnica, medicina ed etica. Prassi del principio di responsabilità*, Einaudi, 1997, p. 122 ss.

[63] P. Stanzione, *La genitorialità tra legittimità, verità e responsabilità*, in *Rass. dir. civ.*, 2019, p. 668 ss.

[64] The topic presents another question: the possibility for biologically male subjects to resort to uterus transplantation to procreate without resorting to a female carrier. This is an issue that brings with it several legal risks. Simplifying, we can say that the most insidious obstacles concern the ethical level, based on the Montreal criteria accepted by the Inter-

genesi […] prospetta una liberazione dai vincoli naturali della fecondazione». It is not easy to provide an answer to all the questions asked. The difficulty mainly concerns cultural differences. On the one hand there is a strong tendency to transform every desire into a right to be claimed, to rely on the goods market to purchase relational goods (care activities), to identify happiness with freedom, on the other hand it is necessary to overcome the ambiguity linked to the notion of person. Being a mere artifact of machines and being a construct of mind and body[65], therefore, living entities[66].

The jurisprudence of the Court of Cassation (case 2019) shows that the French legal system also seems to follow the path that could lead to the elimination of the bans[67]. The solution adopted in France could be imitated by other European legal systems and come closer to the US legal system. It would, however, be desirable for legislators and jurisprudence to appeal not to a universalistic principle, but to a principle of reasonableness, to evaluate case by case, not only what is right, but also what is good, especially for children born with new reproductive techniques.

Maybe we need to find a balance. The world is sospended between utopian and discopian vision of technology. The future may provide us a mixed reality in which it is useful to identify an osmotics relationship between real and virtual. Only in this way the artificial intelligence, robotics and technologies take rights seriously[68].

national Society of Uterus Transplants, which establish that the recipients are "genetically female", thus excluding subjects born as men from this practice, an aspect which has attracted criticism from those who maintain that it is a violation of the right to independent pregnancy of transgender women. V.G. Mookerjee - D. Kwan, *Uterus transplantation as a fertility option in transgender healthcare*, in *International Journal of Transgender Health*, 2020, 21, p. 122 s.; J. Balayla - P. Pounds - A. Lasry, et a., *The Montreal Criteria and uterine transplants in transgender women*, in *Bioethics*, 2021, p. 326 ss.

[65] P.G. Monateri, *The 'Anonymous Matrix' Diritti umani e spazi imperiali nell'era globale*, in *Sovranità e diritti al tempo della globalizzazione*, a cura di G. Contaldi, Roma Tre Press, 2021, p. 55.

[66] G. Teubener, *The Anonymous Matrix: Human Rights Violations by 'Private' Transnational Actors*, in *The Modern Law Review*, 2006, p. 335.

[67] P. Di Nicola, *Arlie Russel Hochschild e la commercializzazione delle emozioni*, in *Sociologia Generale*, eds. R. Bichi, Vita e pensiero, 2022, p. 368 ss.

[68] R. Dworkin, *I diritti presi sul serio*, Bologna, 2010.

VIRTUAL PROPERTY AS A MODERN OBJECTIVE OF PROPERTY LAW: CHALLENGES FOR GEORGIAN LAW

Tamar Zarandia e Giorgi Amiranashvili

1. The rapid development of digital technologies has fundamentally transformed the ways in which individuals create, use, and exchange value. Alongside traditional material assets, a wide range of non-physical resources – such as digital platforms, virtual environments, online accounts, and cryptographic assets – have acquired significant economic, social, and cultural importance. These developments pose profound challenges for property law, which has historically been grounded in the regulation of tangible objects. As a result, modern legal systems are increasingly confronted with the question of whether, and to what extent, virtual objects may constitute legitimate objects of property rights.

In contemporary legal discourse, the concept of *virtual property* has emerged as an attempt to capture this evolving reality. Although intangible assets have long been recognized within legal frameworks – most notably through intellectual property law – the distinctive nature of virtual property resists easy classification. Virtual objects often exist independently of a single legal relationship, are continuously accessible in digital environments, and are subject to complex interactions between users, platform providers, and third parties. These features challenge traditional assumptions about exclusivity, control, and durability that underpin classical property law.

The Georgian legal system, like many civil law systems, formally acknowledges incorporeal property interests. However, the existing doctrinal framework does not clearly address virtual property as a separate and coherent category. This normative gap becomes particularly evident when considering the growing economic value of virtual assets

and the increasing frequency of disputes related to their use, transfer, and protection. Comparative legal developments – especially judicial and legislative approaches adopted in other jurisdictions – demonstrate that the issue of virtual property is no longer theoretical but demands concrete legal solutions.

Against this background, this paper examines virtual property as a modern object of property law, with a particular focus on the challenges it poses for Georgian law. The study aims to clarify the concept of virtual property, distinguish it from other forms of intangible assets, and assess whether existing property law principles are capable of accommodating it. By analyzing doctrinal approaches, comparative jurisprudence, and the relevant provisions of the Civil Code of Georgia, the paper seeks to contribute to the development of a coherent theoretical and normative framework for the protection of virtual property within Georgian private law.

2. At the modern stage of the development of property law, its substantive scope is characteristically expanding. The Civil Code of Georgia understands property as comprising both corporeal things and non-material (intangible) property assets. This alone confirms that the time has passed when property was attributed only to material objects. In contemporary legal literature, there are views that the right of ownership should extend to such incorporeal objects as software[1], the content of websites, and even personal data[2]. Naturally, such an expansion and, even more so, the framing of the issue in relation to personal data, may be debatable. However, when the law is in search of new solutions, when it must adapt to new technologies, any opinion – including one that calls into question the postulates of legal dogmatics – has the right to exist. Such is the demand of legal realism.

As an example, should computer code, which is created and, in fact, is the property of its creator, be protected as property? A large por-

[1] For a discussion on whether so-called software can be attributed to a product, see T. Zoidze, *Compensation for Damage Caused by Defective Products*, Tbilisi, 2016, p. 37 ss.

[2] Cfr. J. Litman, *Information Privacy/Information Property*, in *Stanford law review*, 2000, vol. 52:1283, p. 1290, in *http://www-personal.umich.edu/~jdlitman/papers/infoprivacy.pdf*.

tion of computer code is only one step removed from a simple idea, and such types of code are protected by intellectual property law. However, there exists another type of code, which is rarely considered in technical or legal discussions. These codes operate on the Internet and form the basis of most online resources. Often, these codes themselves constitute the structural parts of the Internet. Domains, websites, emails, and even entire virtual worlds[3] are examples of this second type of code. In many cases, these codes are interconnected and are referred to as virtual property[4].

Generally, we control virtual property through intellectual property law, as both belong to intangible assets[5]. However, the very term "virtual property" is problematic to understand, as this term itself carries many connotations[6], which complicates the definition of its essence. It is known that virtual property is "different", but a precise definition of this distinctiveness does not exist. Consequently, owners of intellectual property are often restricted by contracts known as End-User License Agreements (EULAs). Due to these agreements, distinct protection for virtual rights has not been established in the United States, despite the fact that millions of people and billions of dollars are involved in such transactions. China and Korea have taken significant steps in this direction.

What is virtual property? What is its legal status? What are the means of protecting virtual property? Today, it is highly important that correct approaches towards virtual property exist. Property law seeks to ensure that resources are used in the right direction. In the event that we do not have a theory of virtual property, the use of resources will not be effective. For the development of the internet, the extension of the property regime and the creation of an organization that acts as a regis-

[3] A virtual world can be defined as an alternative, non-physical reality distinct from the actual one.

[4] Cfr. S. van Erp - B. Akkermans, *Cases, Materials and Text on Property Law*, Hart Publishing, 2012, p. 45.

[5] B. Akkermans - E. Ramaekers, *Property Law Perspectives*, Larcier-Intersentia, 2012, p. 10.

[6] Connotative meaning.

trar system for internet addresses proved to be decisive[7]. The regulation of virtual property is also important for the future of the internet. If we protect virtual property, the internet may become a three-dimensional global virtual environment.

The medical, commercial, social, military, and cultural development offered by the virtual environment is not yet well studied. Therefore, we must ensure the protection of virtual property, not only because market systems actively recognize its value, but also because we acknowledge its value for societal development. Ultimately, the development of a theory of virtual property is important for the equilibrium of the law, as it adapts to new concepts[8] and fosters the development of the field in the future. In relation to this issue, an interesting decision is one from the Bonn Court of Second Instance, which recognized a provider's virtual property right over the software of a website[9]. The lawsuit was filed by a participant who was banned from further access to chat rooms. The court's decision discussed the legality of the provider's actions towards a user with whom no contract had been concluded. The court found possible legal grounds for the expulsion from the chat in Paragraph 1004 of the German Civil Code (BGB)[10], assuming that the provider has a "virtual right" of property inviolability (virtuelles Hausrecht), which consists of the right to use the software hosted on the server for appropriate purposes (to protect its own rights).

The court ultimately qualified the right to use the software as "virtual property" (virtuelles Eigentum) and granted the defendant the

[7] International Corporation for Assigned Names and Numbers.

[8] Cfr. S. van Erp - B. Akkermans, *Cases, Materials and Text on Property Law*, cit., p. 45 s.

[9] Vgl. LG Bonn, MMR 2000, 109, quoted in: E.A. Войниканис - М.В. Якушев, Информация. Собственность. Интернет. Традиции и новеллы в современном праве, Волтерс Клувер, 2004, p. 31.

[10] §1004. Claim for removal and injunction (1) If the ownership is interfered with by means other than removal or retention of possession, the owner may demand that the disturber remove the interference. If there is the concern that further interferences will ensue, the owner may seek a prohibitory injunction. (2) The claim is excluded if the owner is obliged to tolerate the interference. Cfr. J. Kropholler, *German Civil Code: Study Commentary*, Tbilisi, 2014, p. 726.

corresponding right of protection. According to the court's opinion, the plaintiff – the expelled participant from the chat – had voluntarily bound themselves to participation in the chat by consent. On the other hand, the party that permitted its use of the chat without additional conditions (i.e., the provider) was not entitled to arbitrarily terminate such use. However, the court here defined the conditions that could have been additionally established by the provider (which would have given it freedom of action), and the restrictions whose legality is linked to the reactions of other participants. Thus, as follows from the court decision, "virtual property" is characterized not primarily by the possibility of preventing any infringement (as is the case with classical property), but rather its structure is directly linked to the expectations of participants in an open communication process; i.e., from the outset, it is connected to the right of third parties to use it[11].

3. Virtual property is characterized by exclusive attribution, meaning that if one person is the owner, they may prohibit others from possessing it and from engaging in any unauthorized acts. Virtual property possesses a durable, fixed nature, which implies that it exists independently of its owner and does not require activation through computer hardware or software to become accessible. According to its final characteristic, code, as an object of property, is perfected by its interconnectedness, thereby enabling a broad range of persons to interact with it, and it is not stored solely for one individual, nor solely on that individual's hard drive. Consequently, these three components determine the recognition of virtual property and the extension of property rights over it, meaning that any other code which does not satisfy these components should not be considered as virtual property[12].

Therefore, virtual property may include websites, components of virtual worlds and computer games, books, music, and films hosted online as digital files, rather than the copyright/related rights associated

[11] Cfr. Е.А. Войниканис - М.В. Якушев, Информация. Собственность. Интернет. Традиции и новеллы в современном праве, cit., p. 32.

[12] G. Zhorzholiani, *Virtual Property as an Object of Property Law*, *Georgian-German Journal of comparative law*, 2019, n. 3, p. 27 s.

with them, and finally, cryptocurrency. However, it should be noted that this list is not exhaustive[13].

Virtual property, of course, cannot be equated or fully placed on the same level as traditional objects of property law. However, justifying this view and completely separating virtual property from property law would, for any legal system – be it common law or civil law – leave virtual property unprotected, which would clearly be unjustified. Consequently, all prerequisites that establish property rights in the physical world should be considered for virtual property as well[14].

The absence of a physical element should not serve as grounds for denying virtual property the status of property. On the contrary, in such cases, the social and economic benefit contributed by virtual property should outweigh the limitation of recognizing only movable or immovable – that is, physical – objects as property. Therefore, virtual property must be protected in the same manner as any property existing in the physical world. The substantive characteristics of virtual property under common law property principles, in turn, are mirrored in the content of property rights in Georgia through the concepts of exclusivity and free enjoyment[15].

Regarding property, it should be noted that Article 147 of the Civil Code of Georgia includes incorporeal property interests, which should not be confused with virtual property. This is because Article 152 of the Civil Code specifies that incorporeal interests consist solely of claims and rights[16].

4. The transformation of social and economic relations through digital technologies has exposed the limitations of traditional property law concepts that are primarily oriented toward tangible objects. As this paper has demonstrated, virtual property has evolved into an independent and economically valuable category of assets whose legal treatment can no longer be adequately addressed solely through existing doctrines

[13] *Ibidem*, p. 28.
[14] *Ibidem*.
[15] *Ibidem*, p. 29.
[16] *Ibidem*.

of intellectual property or contractual regulation. The growing significance of virtual environments, digital platforms, and cryptographic assets requires property law to reassess its foundational assumptions regarding materiality, exclusivity, and control.

The analysis shows that virtual property possesses distinctive characteristics – exclusive attribution, durability, and interconnectedness – that justify its recognition as a legitimate object of property rights, albeit not identical to classical corporeal property. Comparative legal developments in foreign jurisprudence illustrate that legal systems are already adapting property law concepts to the digital sphere. These developments confirm that virtual property is not merely a theoretical construct but a practical legal reality demanding coherent protection.

Within the Georgian legal system, the inclusion of incorporeal property interests in the Civil Code provides an important doctrinal foundation; however, it remains insufficient to fully capture the specific nature of virtual property. The current framework, which limits incorporeal interests largely to claims and rights, leaves significant uncertainty regarding the legal status, transferability, and protection of virtual assets. This normative gap risks undermining legal certainty and the effective use of digital resources in an increasingly virtualized economy.

Accordingly, the paper concludes that Georgian property law should move toward the explicit recognition of virtual property as a distinct object of property rights, while adapting classical property principles to its unique characteristics. Such development would not only enhance legal protection and predictability but also support technological innovation and societal development. Ultimately, the evolution of virtual property doctrine represents a necessary step in maintaining the coherence and relevance of property law in the digital age.

ALGORITHMS, WORK AND NEW SOCIAL RIGHTS IN THE DIGITAL ERA

ALGORITHMIC TRANSPARENCY AND THE PROTECTION OF RIGHTS IN CYBERSPACE

Denisa Rudžiková

1. Labour relations have historically developed as a distinct area of law responding to the imbalance of power between the employer and the employee. From their inception, their protective function has been based on the assumption that decision-making concerning the rights and obligations of the individual is the result of human assessment that can be retrospectively identified, reasoned, and subjected to legal review. This assumption did not represent merely a technical framework for decision-making, but a fundamental normative pillar through which labour law limited the exercise of power and ensured the protection of the weaker party to the employment relationship.

The development of digital technologies and the use of algorithmic systems in the field of work management are gradually undermining this pillar. Decision-making processes that were traditionally linked to identifiable human actors and situated within the organisational structures of the workplace are moving into cyberspace – a digital space in which the exercise of decision-making power is mediated by technical infrastructure, data flows, and automated information processing. In this environment, algorithmic systems become part of decision-making on issues that have traditionally been subject to labour law protection,

thereby changing the fundamental assumptions of the legal control of such decisions[1].

Cyberspace therefore, in the context of labour relations, does not represent merely a new environment for their realisation, but also a new space for the exercise of power. Decision-making in the digital space is characterised by a high degree of technical mediation, automation, and scalability, as a result of which it becomes detached from direct human interaction. The exercise of power shifts from personalised decisions to systems based on the processing of large volumes of data and the statistical evaluation of behavioural patterns, which fundamentally alters its legal comprehensibility and the traditional assumptions of legal control[2].

It is precisely in this context that algorithmic decision-making acquires particular legal significance. Decisions taken or mediated by algorithmic systems are capable of systematically shaping an individual's position under labour law without traditional forms of reasoning and without clear attribution of responsibility. Thus, cyberspace becomes a space in which power over an individual's working life is exercised in a manner that raises fundamental questions about the legitimacy of decision-making and the preservation of effective legal protection. The aim of this contribution is to analyse how algorithmic decision-making

[1] The literature on algorithmic management and algorithmic decision-making in labour-related contexts is extensive. This contribution necessarily limits itself to a selected number of representative works. See, inter alia, M. Dolobàč - E. Lackovà, *Futurology of labour law*, Leges, 2022, p. 60; A. Keegan - J. Meijerink, *Algorithmic Management in Organizations? From Edge Case to Center Stage*, in *Annual Review of Organizational Psychology and Organizational Behavior*, 2025, p. 397 ss.; N. Jabagi - A.M. Croteau - L.K. Audebrand - J. Marsan, *Do algorithms play fair? Analysing the perceived fairness of HR decisions made by algorithms and their impacts on gig workers*, in *International journal oh human resource management*, 2025, p. 240; S. Herath Pathirannehelage - Y.R. Shrestha - G. Von Krogh, *Design principles for artificial intelligence-augmented decision making,* in *European journal of informatio system*, 2025, p. 210 ss.; M. Giaconi - L. Giasanti - S. Varva, *Labour Law and Effectiveness of EU Anti-Discrimination Legislation on the Grounds of Disability during the Recruitment Process: The Case of the Genetic Features*, in *Revija Kopaoničke škole prirodnog prava*, 2025, p. 16.

[2] E. Lackovà, *Fragility of pre-contractual labour relations in the light of algorithmic recruitment*, in *Diritto lavori mercati*, 2022, p. 72 ss.

carried out in the environment of cyberspace alters the fundamental assumptions underlying labour-law protection. The contribution is based on the premise that algorithmic decision-making in the digital space does not constitute merely a technical innovation, but rather a legally relevant phenomenon that calls for a reassessment of traditional concepts of legal control over the exercise of power. In this context, it examines the extent to which European Union law is capable of ensuring, through transparency, the legal comprehensibility and effective control of decision-making power exercised in this manner.

2. Algorithmic decision-making in labour relations does not represent merely a new technical tool for the management of work, but a specific mode of exercising decision-making power, whose legal significance lies primarily in its normative effects. Algorithmic systems today function not only as tools supporting human decision-making, but as mechanisms through which decisions on access to work, an individual's position under labour law, performance evaluation, or further professional development are systematically shaped. The legal relevance of algorithmic decision-making therefore does not lie in the automation of decision-making processes as such, but in the fact that its outputs are capable of determining legally significant situations without direct, individually addressed human intervention and without traditional forms of reasoning[3].

From an analytical perspective, it is therefore necessary to understand algorithmic decision-making as a multi-layered process in which normatively relevant decisions are already taken at the individual stages of its operation. At the input stage, data that are considered legally and organisationally relevant are selected and structured. These decisions, although often presented as technical or neutral, in fact determine which aspects of an individual's work performance, behaviour,

[3] See, inter alia: M. Bastida - A. Vaquero Garcìa - M.Á. Vazquez Taìn - M. Del Rìo Araujo, *From automation to augmentation: Human resource's journey with artificial intelligence*, in *Journal of industrial information integration*, 2025, vol. 46, p. 2; E. Albaroudi - T. Mansouri - A. Alameer, *A Comprehensive Review of AI Techniques for Addressing Algorithmic Bias in Job Hiring*, in *AI*, 2024, vol. 5, p. 390 ss.

or personal profile will be subject to assessment and which will remain outside the decision-making framework. In the subsequent stage of algorithmic processing, these inputs are transformed into models, scores, or categories that serve as the basis for further decision-making. The output stage then generates recommendations or decisions that are in practice often implemented directly, whether this involves the exclusion of a job applicant, a reduction in performance evaluation, or restrictions on access to work tasks[4].

It is precisely this multi-layered structure that constitutes a particular challenge for labour-law protection. Whereas traditional labour law proceeded from an understanding of a decision as a one-off act attributable to a specific decision-maker, algorithmic systems produce legally significant outcomes as the cumulative effect of multiple partial decisions dispersed across time and space. Interference with an individual's position under labour law is therefore often not the result of a single identifiable act, but the consequence of the repeated application of a decision-making model that systematically favours certain profiles while excluding others. The exercise of decision-making power thus shifts into digitally mediated processes carried out through technical infrastructure and data flows, rather than through direct interaction between the parties to the labour-law relationship. Algorithmic decision-making therefore becomes the dominant form of the exercise of labour-law power in the digital space (cyberspace), in which the traditional assumptions of legal control and responsibility are fundamentally weakened.

A particular problem of the exercise of decision-making power as thus transformed is the normative opacity of algorithmic decision-making. This does not concern merely the technical difficulty of understanding how algorithmic systems operate, but above all the absence of an intelligible and legally relevant reasoning that could be subjected to normative assessment. The individual thus becomes the addressee

[4] See, inter alia: A. Kelly-Lyth, *Algorithmic discrimination at work*, in *European labour law journal*, 2023, vol. 14, p. 152 ss.; Z. Chen, *Ethics and discrimination in artificial intelligence-enabled recruitment practices*, in *Humanities and social sciences communications*, 2023, p. 567.

of decisions with significant legal consequences without being able to identify the reasons on the basis of which their position under labour law has been determined. Externally, the decision appears as an objectified outcome of the system, while its normative grounds remain encoded in data models, weightings, and threshold values that elude traditional forms of legal control[5].

The opacity of algorithmic decision-making at the same time creates structural conditions for the emergence of discriminatory effects. Algorithmic systems are typically trained on historical data that reflect existing inequalities in the labour market, such as occupational segregation, gender-based pay disparities, or the systematic disadvantage of certain groups of workers. If these data patterns are not critically examined, algorithmic systems do not merely reproduce them passively, but may also amplify them. Discriminatory effects therefore generally do not arise as a result of the explicit consideration of protected characteristics, but rather through ostensibly neutral criteria that are closely correlated with them[6].

A further risk of these discriminatory effects lies in their indirect and often difficult-to-identify nature. Decisions based on scores, categories, or predictions of future behaviour may lead to the systematic exclusion of certain individuals from employment opportunities without it being clear on the basis of which criteria such exclusion occurs. Discrimination thus does not manifest itself as an isolated failure, but as the cumulative effect of the repeated application of decision-making models that, over time, shape entire categories of workers. The appearance of objectivity, efficiency, and technological neutrality thereby ob-

[5] M. Fabris - N. Baranowska - M.J. Dennis - D. Graus - P. Hacker - J. Saldivar - F.Z. Borgesius - A.J. Biega, *Fairness and Bias in Algorithmic Hiring: A Multidisciplinary Survey*, in *ACM Transactions on intelligent system and technology*, 2024, p. 7; S. Chesterman, *Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity*, NUS Law Working Paper Series, 2020, n. 11, p. 4.

[6] S. Milano - C. Prunkl, *Algorithmic profiling as a source of hermeneutical injustice*, in *Philosophical Studies*, 2024, vol. 182, p. 188; J. Kiesse Bahangulu - L. Owusu - Berko, *Algorithmic bias, data ethics, and governance: Ensuring fairness, transparency and compliance in AI-powered business analytics applications*, in *World journal of advanced research and reviews*, 2025, vol. 25, p. 1748.

scures the fact that such decision-making entails significant normative consequences.

At the same time, the opacity of algorithmic systems fundamentally complicates the identification and substantiation of discriminatory effects. Traditional mechanisms of protection against discrimination are based on the possibility of comparing the treatment of individuals and identifying the criteria that led to different outcomes. In the context of algorithmic decision-making, however, the affected person generally lacks access to information about the data used, the logic of the decision-making process, or the weighting of individual factors. As a result, the burden of proof is significantly complicated in practice, thereby weakening the real enforceability of existing protective mechanisms[7].

These characteristics fundamentally call into question the ability of traditional labour-law and anti-discrimination instruments to ensure effective protection of the individual in digitally mediated decision-making processes. From a legal-theoretical perspective, algorithmic decision-making therefore does not constitute merely a new technological challenge, but an intervention into the very foundations of labour-law protection. The question thus remains open as to which legal means and through which regulatory strategies European Union law seeks to respond to these challenges.

3. The issue of algorithmic decision-making in labour relations has not developed in European Union law as an isolated labour-law problem, but rather as part of a broader reflection on the implications of artificial intelligence for the exercise of decision-making power in the digital space. Its legal conceptualisation has therefore taken place in parallel at several levels – through strategic and policy-oriented documents as well as through binding legal acts – which have mutually influenced one another and gradually shaped the normative framework for the regulation of algorithmic systems.

[7] A. Alacovska, *Algorithmic Paranoia: Gig Workers' Affective Experience of Abusive Algorithmic Management*, in *New technology, work and employment*, 2024, p. 422 ss.; see also D. Rudžiková, *Vplyv AI na pracovné právo*, in *Inovatívne právo a inovácie v práve*, Univerzita Pavla Jozefa Šafárika v Košiciach, 2024, p. 31 ss.

The foundational normative questions associated with algorithmic decision-making began to be more explicitly reflected in the European context within the framework of the so-called European approach to artificial intelligence. Already, the Communication from the Commission Artificial Intelligence for Europe (2018), followed by the Ethics Guidelines for Trustworthy AI prepared by the High-Level Expert Group, identified key risks of automated decision-making, in particular the opacity of decision-making processes, the possibility of systematic biases, and the weakening of legal control in areas with significant impacts on individuals, including the labour market. In these documents, artificial intelligence is understood not only as a technology with innovative potential, but also as a phenomenon that requires particular legal attention wherever automated systems replace or substantially modify human decision-making.

These conceptual foundations were further developed in the subsequent years through additional strategic initiatives of the European Union, in particular the *White Paper on Artificial Intelligence* (2020), which accompanied the gradual formation of binding legal regulation of artificial intelligence. They therefore cannot be understood merely as a preliminary stage preceding legal regulation, but rather as an integral part of a dynamic regulatory process in which normative reflections on the risks of algorithmic decision-making were progressively translated into legally binding rules. This development indicates that the regulation of algorithmic decision-making in the European Union emerges as a response to identified systemic risks associated with the digitally mediated exercise of power, rather than as an isolated legislative intervention.

This process acquires particular significance in the field of work, where algorithmic systems increasingly enter into decision-making concerning access to employment, the evaluation of work performance, the allocation of work tasks, or the continuation of labour-law relationships. In this context, general considerations relating to artificial intelligence are translated into specific labour-law issues concerning the protection of the weaker party, equal treatment, and the reviewability of decisions in a digitally mediated environment.

Binding legal acts of the European Union – most notably the Artificial Intelligence Act, the General Data Protection Regulation, and the specific legal framework governing platform work – represent distinct yet interconnected regulatory responses to these challenges. Their relationship, however, cannot be understood as uniform, either in terms of their normative foundations or the temporal context of their adoption. For this reason, the chapter first focuses on the Artificial Intelligence Act as the core regulatory framework that systematically addresses the risks of algorithmic decision-making through a risk-based approach, and subsequently examines the role of the General Data Protection Regulation and the specific legal regulation of platform work as complementary, or application-oriented, layers of protection in the field of labour-law relations.

3.1 The Artificial Intelligence Act constitutes the core legal framework through which the European Union responds to the risks associated with algorithmic decision-making in the digital space. In the field of work, it acquires particular significance by classifying algorithmic systems used in recruitment, evaluation, the management of work performance, or the allocation of work tasks as high-risk systems. Through this classification, the law explicitly acknowledges that these are systems through which decision-making power is exercised with the potential to substantially affect the labour-law position of individuals[8].

The AI Act is based on the assumption that the risks of algorithmic decision-making cannot be effectively addressed solely through ex post control of individual decisions. Regulatory emphasis is therefore shifted to the stages of design, development, and deployment of algorithmic systems. The concept of high-risk systems is grounded in the idea that a higher degree of interference with individual rights must be balanced by increased obligations and responsibility on the part of the entities that develop, place on the market, and use such systems.

The obligations attached to high-risk algorithmic systems therefore primarily concern risk management, the quality and appropriateness of

[8] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) - See Article 6(2) AI Act and Annex III, point 4.

the data used, documentation of the system's functioning, its ongoing monitoring, and the possibility of intervening in its operation. This regulatory approach reflects the fact that decision-making mediated by algorithmic systems is the outcome of a complex process in which normatively relevant choices are made even before the system is applied to an individual case. Legal control is thus directed primarily at the conditions under which algorithmic systems are developed and used, rather than at the individual decisions that result from their operation.

A particular role in this context is played by the requirement of human oversight. As a corollary of this system-oriented regulatory design the AI Act assumes that algorithmic systems with significant legal effects should not function as autonomous decision-making mechanisms enclosed within technical infrastructure. Oversight is intended to ensure that decision-making processes remain traceable, comprehensible in their basic features, and, where necessary, correctable. However, this requirement is likewise conceived primarily as an obligation imposed on the entities that design and use such systems, rather than as an individual right of the persons directly affected by algorithmic decision-making.

Regulation conceived in this manner demonstrates that the AI Act rejects the understanding of algorithmic decision-making as a completely inaccessible "black box" and establishes the basic conditions for the safe and controllable exercise of algorithmic power in the digital space. At the same time, however, it reveals the limits of a systemic approach based on preventive risk regulation. Within the framework of the AI Act, the intelligibility and controllability of algorithmic systems are linked primarily to the obligations of providers and users of high-risk systems and to oversight by the competent public authorities, while the procedural position of the individual whose labour-law status is affected by algorithmic decision-making remains addressed only to a limited extent.

These limitations become particularly evident in situations in which algorithmic decision-making is applied directly to individual workers, especially in the context of digital labour platforms. It is precisely here that it becomes apparent that systemic risk regulation, although nec-

essary, is not sufficient in itself to ensure effective individual legal protection, thereby opening the space for supplementary regulatory mechanisms focused on the procedural position of the persons concerned.

3.2 The platform environment represents a distinct segment of the digital space in which algorithmic decision-making is applied in a concentrated and intensive manner. In this environment, the performance of work is mediated from the outset by digital infrastructure and data flows, while decisions concerning the allocation of work, the evaluation of work performance, the imposition of sanctions, or the termination of cooperation are to a large extent automated. Algorithmic systems here do not merely perform a supportive function in the organisation of work, but act as the central mechanism for the exercise of decision-making power in digitally mediated labour relations, thereby largely replacing traditional forms of organisational, managerial, and disciplinary power.

This concentration of decision-making power in digital systems simultaneously accentuates the structural asymmetry of power and information between the platform and the worker. The platform exercises control over the algorithmic systems, the rules governing their operation, as well as the data that enter into decision-making processes. The worker, by contrast, is exposed to decisions with an immediate impact on their work opportunities, income, and position on the platform, which are generated within an environment whose internal logic and evaluative criteria are generally not accessible to them.

These specific features are addressed by Directive (EU) 2024/2831 of the European Parliament and of the Council on improving working conditions in platform work, adopted in 2024. The Directive devotes particular attention to algorithmic management of work in Chapter III, thereby explicitly qualifying algorithmic systems as legally relevant instruments of work management, rather than as a neutral technical background to labour-law relations.

A central element of this regulation is the platform's duty to inform workers. The platform has an active obligation to inform the worker that their work is managed or influenced by automated systems, as well

as about the nature of those systems. The worker must be informed about the use of automated decision-making or monitoring, the types of decisions taken by algorithmic systems – such as the allocation of work tasks, performance evaluation, the imposition of sanctions, or account deactivation – as well as the main factors influencing those decisions. The purpose of this information obligation is not merely the formal fulfilment of a notification requirement, but to enable at least a basic understanding on the part of the worker of the digitally mediated exercise of decision-making power.

This obligation is complemented by the requirement to disclose clear rules governing the functioning of algorithmic management of work. Although the Directive does not require access to the source code of algorithmic systems, it does impose an obligation on platforms to disclose the criteria on the basis of which algorithms allocate work, assess workers' performance, and apply sanctions or restrictions. This approach seeks to limit situations in which workers are exposed to the consequences of algorithmic decision-making without being able to understand which forms of behaviour or circumstances lead to an improvement or deterioration of their position at work.

A particularly significant intervention in algorithmic management of work is the explicit prohibition of the monitoring and processing of certain categories of sensitive personal data. The Directive prohibits, in particular, the monitoring of workers' emotional or psychological states, the processing of biometric data, the analysis of health status, and the monitoring of private communications. In this way, European Union law sets substantive limits on algorithmic management of work and rejects its extension into areas that would lead to a disproportionate interference with workers' human dignity and privacy in the digital working environment.

A key element of the regulatory framework is, finally, the requirement of human oversight and the possibility of reviewing algorithmic decisions. The Directive requires that decisions with a significant impact on a worker's position under labour law must not be subject exclusively to automated processing. Workers must have the possibility to request an explanation of a decision, to lodge an objection, and to

obtain a review by a qualified person. An algorithmic decision should therefore not assume the character of a final and unreviewable act[9].

The significance of Chapter III of the Platform Work Directive lies in the fact that it explicitly qualifies algorithmic systems as instruments of work management and attaches specific labour-law obligations to their use. This framework may be read as a systematic shift in the normative understanding of algorithmic management of work, insofar as part of the informational and responsibility-related burden is transferred to platforms as the entities that use these systems. At the same time, this creates a normative linkage between labour-law protection and data protection in the context of the digitally mediated exercise of decision-making power.

The foregoing analysis indicates that the regulation of algorithmic decision-making in the field of work within European Union law is shaped primarily as a regulation of the systemic conditions under which digitally mediated decision-making power operates. Both the Artificial Intelligence Act and the specific legal framework governing platform work respond to the risks of algorithmic management of work mainly by imposing obligations on the entities that design, deploy, and operate algorithmic systems, with emphasis placed on the organisational, technical, and procedural aspects of their functioning.

However, the question of the procedural position of the individual as the addressee of automated decision-making is not exhausted within the framework of sector-specific labour-law regulation in European Union law, but is necessarily linked to the general framework governing the processing of personal data, which approaches these decision-making processes from a different normative perspective.

3.3 In a digitally mediated working environment, the processing of personal data is an integral part of algorithmic decision-making. Algorithmic systems used in the management of work operate on the basis of the systematic collection and evaluation of data relating to individuals, which serve as the basis for decisions with significant legal conse-

[9] Directive (EU) 2024/2831 of the European Parliament and of the Council on improving working conditions in platform work. See Chapter III, Articles 7–11.

quences. The regulation of personal data processing therefore, in this context, goes beyond the traditional understanding of the protection of privacy and assumes the significance of an instrument of procedural control over the exercise of decision-making power in the digital space.

The General Data Protection Regulation responds to the risks of automated decision-making through a specific provision in Article 22, which establishes limitations on decisions based solely on automated processing, including profiling, where such decisions produce legal effects or similarly significantly affect the data subject. The procedural dimension of the protection of the individual is subsequently developed primarily through the right of access to data under Article 15, which grants the data subject the right to obtain information about the existence of automated decision-making, as well as to receive at least meaningful information about the logic involved, the significance, and the envisaged consequences of such processing for the data subject[10].

The scope and content of these procedural rights have long been the subject of interpretative disputes, in particular with regard to the question of the extent to which they give rise to an obligation to provide the data subject with an explanation of a specific automated decision. A significant development in this respect occurred in the case law of the Court of Justice of the European Union, most notably in its judgment in Case C-203/22 *CK v Magistrat der Stadt Wien*. In that judgment, the Court interpreted the concept of *"meaningful information about the logic involved"* as meaning that the data subject has the right to request an explanation of the principles and procedures applied in the automated processing of their personal data for the purpose of achieving a specific outcome. Such an explanation must be provided in a concise, intelligible, and accessible form and must make it possible to understand how the data subject's data were used in their individual case[11].

This interpretation goes beyond an understanding of information obligations as a purely formal instrument and points to the significance

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). See Articles 15 and 22.

[11] Judgment of the Court of Justice of 27 February 2025, *Case C-203/22.*

of the procedural rights of the data subject in the context of automated decision-making. At the same time, it shows that the protection provided by the GDPR is linked to the regulation of the processing of personal data and therefore focuses primarily on the individual level of the relationship between automated decision-making and the data subject.

The GDPR thus represents, within the system of European Union law, a general framework of procedural protection of the individual in relation to the automated processing of data on which algorithmic decisions are based. This perspective differs from the approaches of the Artificial Intelligence Act and the specific legal framework governing platform work, which primarily regulate the systemic conditions of the exercise of algorithmic decision-making, and creates space for further analysis of issues that go beyond the scope of personal data protection.

4. The analysis of the legal frameworks of the European Union responding to the use of algorithmic systems in the field of work points to the existence of a common normative core that connects these frameworks despite their differing regulatory approaches, techniques, and addressees. The individual legal acts operate with different concepts, intervene at different stages of the algorithmic decision-making process, and impose obligations on different actors. What these approaches nevertheless have in common is the effort to ensure that decision-making mediated by algorithmic systems remains legally comprehensible, reviewable, and compatible with the fundamental rights of the individual. In this context, transparency appears as a normative concept through which this shared regulatory ambition can be systematically captured and explained, while at the same time constituting a key precondition for the protection of the individual in the environment of cyberspace.

Transparency in this article is not understood as a technical property of algorithmic systems nor as a requirement of full disclosure of their internal mechanisms. Rather, it is a normative quality of the decision-making process that makes it possible to identify that a decision with significant legal consequences has been taken through algorithmic data processing and, at the same time, to understand the basic

reasons and criteria on which that decision is based. Transparency in this sense constitutes a fundamental protective condition for the legal comprehensibility of algorithmic decision-making, that is, the ability to subject it to legal assessment in terms of legality, proportionality, and compliance with the principle of equal treatment.

The significance of transparency is most clearly manifested in relation to the position of the individual as the addressee of algorithmic decision-making. Decisions adopted in a digitally mediated working environment often have an immediate and substantial impact on individuals' work-related and life opportunities, while arising from processes that, in the absence of specific legal safeguards, remain factually inaccessible to the persons concerned. In this context, transparency does not represent merely an informational standard, but a mechanism for safeguarding the legal position of the individual in cyberspace, as it creates a minimum epistemic framework enabling the nature of the decision to be recognised, its basic logic to be understood, and legally relevant means of protection to be exercised against it. Without such transparency, the exercise of fundamental rights – particularly the right to effective legal protection and protection against discrimination – is reduced to a formal declaration devoid of real normative content.

Particular attention in this context deserves the scope of transparency ensured by the Artificial Intelligence Act. Although the AI Act introduces extensive obligations in the areas of documentation, information provision, and the assurance of human oversight over high-risk algorithmic systems, its regulatory framework is conceived primarily at the level of systemic control of the functioning of these systems. Transparency within the meaning of the AI Act is aimed primarily at ensuring the safety, traceability, and controllability of algorithmic decision-making through obligations imposed on providers and users of high-risk systems and through oversight by competent public authorities, rather than at protecting the individual legal security of the person whose legal position is affected by an algorithmic decision. The Regulation thus does not explicitly construct a subjective right of the individual to an explanation of a specific decision that directly concerns them. This conceptual distinction points to the difference between systemic trans-

parency of algorithmic systems and procedural transparency in relation to the individual as the addressee of a decision, and at the same time explains why the protection of the individual against algorithmic decision-making in the field of work cannot be ensured through the AI Act as such, but requires supplementation by additional legal mechanisms.

Transparency is at the same time of fundamental importance for the functioning of law itself under conditions of the digitalisation of decision-making. Algorithmic systems shift the exercise of decision-making power into digitally mediated processes in which traditional mechanisms of legal control encounter their structural limits. Legal regulation that is unable to ensure even a minimum level of transparency of these processes loses its capacity to effectively regulate the exercise of power that algorithmic systems in fact perform, and thus also its capacity to guarantee the security of the individual in the digital space. Transparency therefore becomes a basic condition for preserving the reviewability of decisions and an indispensable instrument of legal control over power in the environment of cyberspace.

From this perspective, transparency may be understood as one of the fundamental normative requirements for the protection of the individual under conditions of digitally mediated decision-making. Although it is not formulated in European Union law as an autonomous fundamental right, it constitutes a necessary precondition for the exercise of several fundamental rights and functions as their connecting element in the context of algorithmic decision-making in the field of work. Transparency in this sense operates as a legal guarantee of the security of the individual in cyberspace, as it makes it possible to preserve the compatibility of algorithmic decision-making with the fundamental principles of the rule of law. This normative shift towards the transparency of algorithmic decision-making is not limited to binding legal acts, but is also manifested in instruments of soft law through which the regulatory ambitions of the European Union in the field of artificial intelligence are further specified. These instruments confirm that the transparency of algorithmic systems is perceived as a necessary precondition for their legitimate and controllable use in the digital space.

An example is the *Code of Practice for General-Purpose AI Models-Transparency Chapter*, adopted in connection with the Artificial Intelligence Act, which is based on the premise that, without sufficient transparency, neither effective oversight of algorithmic systems nor their responsible use in application contexts with significant impacts on individuals' fundamental rights can be ensured. Transparency is thus confirmed as a normative condition for the legal control of algorithmic decision-making and the protection of the individual, thereby clearly emerging as a requirement that is taking shape across various regulatory instruments of European Union law.

5. Algorithmic decision-making in the field of work represents a qualitative change in the exercise of decision-making power, which is increasingly carried out through digitally mediated processes. As the analysis of the legal frameworks of the European Union has shown, the legal response to this shift does not take the form of a single, unified regulatory instrument, but rather of several partial legal regimes that intervene at different stages of algorithmic decision-making and address different aspects of its risks. Despite this fragmentation, the common denominator of European regulatory approaches is the effort to preserve the legal comprehensibility of decisions with significant consequences for an individual's position under labour law. In this context, transparency does not appear as a purely technical or formal requirement, but as a normative condition for the exercise of legal control over decision-making power that is being transferred into the digital space. At the same time, it becomes apparent that transparency in current European Union law is conceived primarily at the systemic level, while the position of the individual as the addressee of algorithmic decision-making remains protected only partially. If transparency is to function as a genuine instrument of protection, it must enable not only formal information, but also a real understanding of the basic logic of the decision in the individual case. Without such comprehensibility, the individual remains an object, rather than a subject, of algorithmically mediated exercises of power. The future development of European Union law should therefore focus on strengthening transparency vis-à-vis the indi-

vidual as a practically applicable instrument for the protection of rights. Only then can transparency fulfil its function as a legal guarantee of control over the exercise of power in the environment of cyberspace and support the protective character of labour law in the digital age.

ACCOUNTABILITY ALGORITMICA E NUOVI DIRITTI DIGITALI DEI LAVORATORI CONTRO LA DISCRIMINAZIONE AUTOMATIZZATA

Eva Lacková

1. L'intelligenza artificiale (IA) e gli algoritmi rappresentano tecnologie dagli effetti molteplici: non costituiscono di per sé strumenti di disuguaglianza, ma neppure una garanzia di neutralità. Il loro impatto – sociale in senso lato e, per quanto qui interessa, nel contesto lavorativo – si modella in base al *design* dei sistemi, al loro grado di trasparenza, alle possibilità di controllo umano e, soprattutto, al quadro normativo che ne definisce limiti e finalità d'uso.

Come ampiamente discusso dalla dottrina interdisciplinare[1] e confermato dai primi orientamenti giurisprudenziali[2], in assenza di garanzie adeguate, l'IA e gli algoritmi tendono a riprodurre pregiudizi storici,

[1] Per tutti v. J. Gerards - R. Xenidis, *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-discrimination Law*, Publications Office of the European Union, 2021; J. Adams-Prassl - R. Binns - A. Kelly-Lyth, *Directly discriminatory algorithms*, in *Modern Law Review*, 2023, 86, n. 1, p. 144 ss.

[2] Nel contesto italiano, ma con la rilevanza europea, la pronuncia Trib. Bologna 31 dicembre 2020 come analizzata, per tutti, da M. Barbera, *Discriminazioni algoritmiche e forme di discriminazione*, in *Labour & Law Issues*, 2021, n. 1, p. 3 ss.; G. Gaudio, *La CGIL fa breccia nel cuore dell'algoritmo di Deliveroo*, in *Rivista italiana di diritto del lavoro*, 2021, n. 2, II, p. 175; S. Borelli - M. Ranieri, *La discriminazione nel lavoro autonomo. Riflessioni a partire dall'algoritmo Frank*, in *Laour. & Law Issues*, 2021, n. 1, p. 20 ss.; M.V. Ballestrero, *Ancora sui rider. La cecità discriminatoria della piattaforma*, in *Labor*, 19 gennaio 2021; M. Biasi, *L'algoritmo di Deliveroo sotto la lente del diritto antidiscriminatorio...e del relativo approccio rimediale*, in *Argomenti di diritto del lavoro*, 2021, n. 3, p. 780 ss., M. Lammanis, *Frank è un falso cieco: l'algoritmo discrimina i riders*, in *Il lavoro nella giurisprudenza*, 2021, n. 5, p. 526 ss. Analogamente, Trib. Palermo 17 novembre 2023.

ad accentuare le disuguaglianze strutturali e a incidere sui diritti fondamentali, in particolare su quelli in materia di *privacy* e di parità di trattamento. Al contrario, quando i sistemi sono progettati nel rispetto dei principi di uguaglianza e trasparenza, essi possono trasformarsi in potenti strumenti di contrasto alle discriminazioni e di promozione dell'equità nei contesti lavorativi[3].

Anche la recente Risoluzione del Parlamento europeo del 17 dicembre 2025 recante raccomandazioni alla Commissione sulla digitalizzazione, l'intelligenza artificiale e la gestione algoritmica sul luogo di lavoro – *Plasmare il futuro del lavoro* (2025/2080 (INL)) – riconosce che, accanto ai rischi, l'IA e i sistemi di gestione algoritmica possono offrire benefici rilevanti, quali l'ottimizzazione dell'organizzazione del lavoro, una maggiore coerenza e obiettività delle decisioni gestionali, nonché il miglioramento della salute e della sicurezza sul lavoro e della soddisfazione dei lavoratori.

La valutazione dei rischi e dei benefici assume particolare rilievo alla luce del fatto che tali sistemi, inizialmente adottati in modo generalizzato dalle piattaforme di lavoro digitali, sono oggi ampiamente diffusi nell'intero mercato del lavoro e che, secondo recenti studi, l'esposizione dei lavoratori alla gestione algoritmica ha la tendenza di aumentare[4],

[3] Ipotesi di G. Gaudio, *Le discriminazioni algoritmiche*, in *Lavoro diritti Europa*, 2024, n. 1, il quale condiziona la possibilità che un maggiore utilizzo di strumenti di *algorithmic management* contribuisca a ridurre il rischio di discriminazioni nell'ambiente di lavoro – rispetto a decisioni assunte esclusivamente da esseri umani – all'esistenza di un quadro regolatorio adeguato ed efficace, già in parte delineato a livello europeo e nazionale. Analogamente, F. Palmirotta, *Disruptive, yet inclusive AI: solution and boundaries from a labour law perspective*, in *Italian labour law e-journal*, 2025, vol. 1, n. 18, p. 83 ss., la quale sostiene la rilettura dell'apertura normativa per l'IA inclusiva del principio di accomodamenti ragionevoli in chiave proattiva e l'applicazione anticipata dei principi di prevenzione in materia di salute e sicurezza sul lavoro.

[4] Le indagini condotte a livello dell'UE evidenziano significative divergenze nella misurazione dell'adozione della gestione algoritmica. In particolare, la European Working Conditions Survey 2024 stima che il 42,3% dei lavoratori dell'UE sia coinvolto in sistemi di gestione algoritmica, con marcate differenze tra Stati membri; l'Eurobarometro riporta una percentuale ancora più elevata (51,3%), mentre la European Survey of Enterprises on New and Emerging Risks 2024 indica una diffusione assai più contenuta tra le imprese (14,5%). A ciò si aggiunge una recente ricerca dell'OCSE, condotta in quattro Paesi dell'UE (Francia, Germania, Italia e Spagna), che ha rilevato come il 79% delle imprese uti-

generando al contempo opportunità di produttività e nuove criticità in termini di relazioni di lavoro, condizioni lavorative e benessere dei lavoratori.

A parere di chi scrive occorre innanzitutto chiarire, sul piano ontologico, cosa si intenda per discriminazione algoritmica e, successivamente, individuare le relative fonti normative, tenendo costantemente presenti i profili di continuità e di differenziazione rispetto alla disciplina generale della tutela antidiscriminatoria.

2. Quando si affronta il tema della discriminazione algoritmica, è innanzitutto necessario sviluppare una maggiore chiarezza concettuale, poiché la terminologia impiegata nei diversi ambiti scientifici non è uniforme.

Nella letteratura informatica e filosofica, il termine *bias* viene impiegato per descrivere le distorsioni, i danni o le ingiustizie generate dai sistemi algoritmici[5]. In ambito giuridico, invece, le distinzioni illecite tra gruppi vengono qualificate come discriminazione, secondo un significato tecnico e normativo[6].

La nozione di *bias* algoritmico ha un significato più ampio e generale, poiché si riferisce a errori sistematici e ripetibili che producono risultati ingiusti, ad esempio favorendo arbitrariamente un gruppo di individui rispetto ad altri[7]. La nozione giuridica di discriminazione, invece, è più circoscritta e riguarda unicamente trattamenti differenziati fondati su fattori protetti dal diritto dell'UE, quali sesso, origine etnica, età, disabilità, religione o orientamento sessuale, ecc. Allo stesso tem-

lizzi almeno uno strumento di gestione algoritmica. V. European Parliamentary Research Service, *Digitalisation, artificial intelligence and algorithmic management in the workplace: Shaping the future of work*, 2025, disponibile online: *https://www.europarl.europa.eu/RegData/etudes/STUD/2025/774670/EPRS_STU(2025)774670_EN.pdf*.

[5] V. per tutti B. Friedman - H. Nissenbaum, *Bias in computer systems*, in *ACM Transactions on information systems,* 1996, vol. 14, n. 3, p. 330 ss.

[6] Della polisemia nell'uso di termini discriminazione algoritmica e *bias* algoritmico da parte del legislatore europeo v. R. Xenidis, *When computers say no: towards a legal response to algorithmic discrimination in Europe*, in B. Brożek - P. Palka - O. Kanevskai, *Research Handbook on Law and Technology*, Edward Elgar Publishing, 2024, p. 222 ss.

[7] B. Friedman - H. Nissenbaum, *Bias in computer systems*, cit., p. 330 ss.

po, dal concetto di *bias* restano escluse le differenziazioni sistematiche finalizzate alla promozione dell'uguaglianza sostanziale, come alcune misure di azione algoritmica positiva, cd. "discriminazione positiva"[8].

Ne consegue che non ogni forma di *bias* algoritmico può essere ricondotta alla discriminazione tutelata dal diritto europeo (così come non ogni discriminazione rappresenta un *bias*). Nell'ambito del diritto antidiscriminatorio dell'UE, infatti, un *bias* algoritmico può dirsi giuridicamente rilevante solo quando ricorrono tre condizioni fondamentali[9]:

a) il *bias* deve produrre un pregiudizio o uno svantaggio nei confronti di individui appartenenti a gruppi protetti;

b) la discriminazione deve manifestarsi in settori rientranti nell'ambito di applicazione del diritto dell'UE, in particolare nel lavoro e nell'accesso a beni e servizi;

c) il trattamento differenziato generato dal sistema algoritmico deve poter essere qualificato, sul piano giuridico, come discriminazione diretta o indiretta, secondo le categorie tradizionali del diritto europeo[10].

Solo i *bias* algoritmici che rispettano questi tre elementi – soggettivo, oggettivo e concettuale – rientrano nel divieto di discriminazione previsto dal diritto UE.

[8] H. Weerts - R. Xenidis - F. Tarissan - H. Palmer Olsen - M. Pechenizkiy, *The Neutrality Fallacy: When Algorithmic Fairness Interventions are (not) Positive Actions*, *2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24)*, 3–6 Giugno, 2024, Rio de Janeiro, Brasil, 2024. Gli autori suggeriscono che gli interventi di equità algoritmica, talvolta qualificati come «azione positiva algoritmica» ai sensi del diritto antidiscriminatorio dell'UE, dovrebbero essere interpretati principalmente come strumenti di prevenzione della discriminazione, piuttosto che come vere e proprie misure di azione positiva.

[9] R. Xenidis, *When computers say no*, cit., p. 225-226.

[10] La definizione di queste fattispecie è contenuta con qualche piccola differenza in un novero di norme sia sovranazionali che italiane: Art. 2, § 2, Dir. 2000/43/CE in materia di discriminazioni per razza e origine etnica; Art. 2, § 2, Dir. 2000/78/CE in materia di discriminazioni per religione, convinzioni personali, handicap, età, tendenze sessuali; Art. 2, § 2, Dir. 2006/54/CE in materia di discriminazioni di genere. Nella disciplina interna di recepimento, v. art. 2 d.lgs. n. 215/2003 in materia di discriminazioni per razza e origine etnica; art. 2 d.lgs. n. 216/2003 in materia di discriminazioni per religione, convinzioni personali, handicap, età, tendenze sessuali; art. 25 d.lgs. n. 198/2006 in materia di discriminazioni di genere; art. 25 d.lgs. 198/2006 Codice delle pari opportunità.

È opportuno evidenziare che molte delle criticità concernenti il potenziale carattere discriminatorio degli algoritmi non sono intrinsecamente proprie delle nuove tecnologie, ma ripropongono problematiche già note e da tempo affrontate dal diritto antidiscriminatorio tradizionale. Per economicità di spazio non si ripercorrono qui le fonti tradizionali del diritto antidiscriminatorio[11], basta menzionare, come noto, che la disciplina generale in materia di non discriminazione si fonda su un articolato quadro normativo multilivello, nel quale si intrecciano fonti sovranazionali, costituzionali e legislative nazionali.

La normativa antidiscriminatoria generale trova l'applicazione nei confronti dei lavoratori ogniqualvolta l'utilizzo di algoritmi decisionali o di controllo incida su aspetti essenziali del rapporto di lavoro (in senso lato) – quali l'accesso all'attività, le condizioni di impiego, l'assegnazione di incarichi, la valutazione della performance, la determinazione dei compensi, l'irrogazione di sanzioni disciplinari o la cessazione del rapporto. Essa opera, in particolare, quando il funzionamento del sistema algoritmico comporta effetti di discriminazione diretta o indiretta,

[11] A livello europeo, uno dei riferimenti principali è l'art. 21 della Carta dei diritti fondamentali dell'Unione europea (CDFUE), che sancisce il divieto generale di discriminazione. La tutela antidiscriminatoria ai sensi dell'art. 14 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) aveva inizialmente una portata limitata, estendendo il principio di non-discriminazione solamente all'esercizio dei diritti garantiti dalla Convenzione. Con il Protocollo aggiuntivo alla CEDU n. 12/2000, entrato in vigore nel 2005, si è stabilito il divieto di discriminazione operante rispetto a ogni diritto previsto dalla legge, a prescindere dall'ancoraggio alle garanzie espressamente previste dalla Convenzione. In ambito interno, la Costituzione italiana afferma l'eguaglianza formale e sostanziale (art. 3) e tutela la parità di genere nei rapporti economici e sociali (art. 37). Il percorso normativo italiano ha conosciuto un progressivo ampliamento delle tutele nel corso degli anni: dallo Statuto dei lavoratori (artt. 8, 15 e 18, l. n. 300/1970) alle leggi in materia di parità di genere (l. n. 903/1977 e l. n. 125/1991), fino al d.lgs. n. 198/2006 (Codice delle pari opportunità). Rilevanti sono inoltre il d.lgs. n. 286/1998 (Testo Unico sull'immigrazione), il d.lgs. n. 215/2003 (attuazione della direttiva 2000/43/CE sulla parità di trattamento indipendentemente da razza e origine etnica), il d.lgs. n. 216/2003 (attuazione della direttiva 2000/78/CE in materia di occupazione e condizioni di lavoro), nonché il d.lgs. n. 5/2010 (attuazione della direttiva 2006/54/CE sul principio di pari opportunità fra uomini e donne in materia di occupazione e impiego). V. per tutti M. Barbera, *Il nuovo diritto antidiscriminatorio. Il quadro comunitario e nazionale*, Giuffrè, 2007.

legati a dati sensibili o a variabili *proxy*, mentre la complessità e l'opacità del processo decisionale impediscono al lavoratore di comprendere o contestare le decisioni che lo riguardano e rappresentano un ostacolo procedurale dell'effettività delle tutele.

In tale contesto, la centralità della trasparenza emerge con particolare forza: nel lavoro "macchiato" di algoritmi, le discriminazioni, pur essendo tecnicamente rilevabili, restano spesso invisibili alla percezione diretta delle vittime[12]. Ne consegue che il semplice divieto di discriminazione non è sufficiente, ma occorre riconoscere diritti complementari che garantiscano informazione, accesso e possibilità di intervento sui processi decisionali automatizzati.

Con specifico riguardo alle discriminazioni algoritmiche diventa, dunque, essenziale osservare con attenzione i recenti sviluppi della legislazione europea in materia di regolazione dell'IA e dei processi decisionali automatizzati, adottando una lente giuslavoristica capace di mettere a fuoco i rischi tecnologici connessi al possibile aggravamento delle disuguaglianze di potere, intrinseche ai rapporti di lavoro. Tale intervento del legislatore europeo – che, per quanto riguarda il rischio discriminatorio derivante dall'uso di algoritmi, non può che non essere considerato più parziale che organico – riflette un consenso generale sul fatto che la normativa vigente possieda un ambito di applicazione materiale sufficientemente ampio da includere la maggior parte dei casi di discriminazione algoritmica[13].

La regolamentazione degli aspetti chiave per la parità di trattamento al lavoro laddove vengono impiegati strumenti di management algoritmico può essere ricondotta al trifoglio di atti normativi europei: il Regolamento UE/2016/679 sulla protezione dei dati (d'ora in poi GDPR), il Regolamento UE/2024/1689 sull'Intelligenza Artificiale (AI Act) e Direttiva UE/2024/2831 sul miglioramento delle condizioni di lavoro nel settore delle piattaforme digitali (Direttiva sulle piattaforme - PWD).

[12] A. Bonezzi - M. Ostinelli, *Can Algorithms Legitimize Discrimination*?, in *Journal of Experimental Psychology: Applied*, 2021, n. 27(2), p. 447.

[13] A. Kelly-Lyth, *Algorithmic discrimination at work*, in *European labour law journal*, 2023, vol. 14, n. 2, p. 166-167.

Il GDPR è un atto normativo di indubbia rilevanza ultranazionale, anche nell'imporre gli obblighi informativi che conducono alla maggiore trasparenza nel trattamento dei dati e profilazione; tuttavia, le sue disposizioni appaiono spesso inadeguate sotto il profilo lavoristico. Un esempio (si può dire ormai "di scuola") indicativo del fatto che il GDPR non è stato concepito come uno strumento di disciplina dei rapporti di lavoro riguarda l'articolo 22, che vieta le decisioni basate esclusivamente su trattamenti automatizzati, comprese quelle fondate su profilazione, qualora producano effetti giuridici o incidano in modo analogo e significativo sull'interessato. Tale divieto, tuttavia, ammette eccezioni fondate su ragioni di necessità contrattuale, ai sensi del paragrafo 2 dello stesso articolo. Questa clausola, pensata in un'ottica generale di tutela dei dati personali, risulta problematica se applicata al contesto lavoristico, dove il consenso del lavoratore e la "necessità contrattuale" non possono essere considerati su un piano di effettiva parità tra le parti, evidenziando così i limiti del GDPR come fonte di garanzia sostanziale nelle dinamiche di gestione algoritmica del lavoro.

A ciò si aggiunge che il requisito della decisione "interamente automatizzata" è stato, per lungo tempo, agevolmente eluso dai datori di lavoro mediante la previsione di un intervento umano meramente formale o qualificando le raccomandazioni algoritmiche come non vincolanti nel processo decisionale. Tale lettura restrittiva dell'art. 22, co. 1, è stata tuttavia in parte ridimensionata dalla giurisprudenza più recente, in particolare dalla pronuncia *Schufa*, che ha contribuito a rafforzare l'interpretazione sostanziale delle tutele previste dalla disposizione[14].

L'AI Act introduce un modello di classificazione dei rischi derivati dall'utilizzo di IA in tutti gli ambiti della vita. I sistemi di intelligenza artificiale che incidono sui diritti dei lavoratori sono classificati come sistemi ad alto rischio ai sensi dell'AI Act, con conseguente applicazione

[14] Sentenza CGUE del 27 febbraio 2025 C-634/21, *Schufa*. Per il valore giuslavoristico della pronuncia v. A. Aza, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context,* in *Industrial law journal*, 2024, vol. 53, n. 4, p. 840 ss.

del relativo regime restrittivo[15]. Rientrano pertanto nella categoria dei sistemi ad alto rischio tutte le applicazioni di IA impiegate in qualsiasi forma di lavoro, subordinato o autonomo, e in tutte le fasi del rapporto – dalla selezione alla gestione fino alla cessazione. Come chiarito dal considerando 57, la *ratio* di tale previsione risiede nel potenziale impatto di questi sistemi sul futuro professionale e sul sostentamento dei lavoratori, nonché sul rispetto dei loro diritti fondamentali. L'uso dell'IA nei processi di assunzione, valutazione o gestione può infatti favorire e consolidare vecchie o nuove forme di discriminazione, rendendo necessarie rigorose garanzie di trasparenza e controllo umano.

In questa prospettiva, ci si può chiedere se e in che misura la recente regolamentazione italiana rifletta e attui tali principi. Da ultimo, la l. n. 132/2025, recante *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, in vigore dal 10 ottobre 2025, definisce i principi generali e l'ambito di applicazione dell'intelligenza artificiale in Italia, promuovendo un uso etico, trasparente e responsabile delle tecnologie digitali, in una prospettiva antropocentrica e in coerenza con il AI Act. Di particolare rilievo per il diritto del lavoro è l'art. 11, co. 3, che impone che l'impiego dell'IA nei processi di organizzazione e gestione del rapporto di lavoro avvenga nel pieno rispetto dei diritti fondamentali e del principio di non discriminazione, escludendo qualsiasi disparità di trattamento fondata su sesso, età, origine etnica, credo religioso, orientamento sessuale, opinioni politiche o condizioni personali, sociali ed economiche, in conformità con il diritto dell'UE. In più, la l. n. 132/2025, se coordinata con le disposizioni del d.lgs. n. 27 giugno 2022, n. 104, cd. Decreto Trasparenza, impone ai datori di lavoro obblighi informativi stringenti sull'uso dei sistemi di IA nei rapporti di lavoro, rendendo strategica l'adozione di *policy* aziendali strutturate per garantire trasparenza.

[15] L'Allegato III, richiamato dall'articolo 6, paragrafo 2, individua tra questi, in particolare: a) i sistemi di IA utilizzati nei processi di assunzione o selezione del personale, compresi quelli impiegati per la pubblicazione di annunci mirati, l'analisi o il filtraggio delle candidature e la valutazione dei candidati; b) i sistemi destinati a decisioni sulla gestione del rapporto di lavoro, quali promozioni, assegnazione di compiti, monitoraggio delle prestazioni o cessazione del rapporto, basate su dati comportamentali o caratteristiche personali.

L'approccio decisamente più settoriale è stato adottato nella redazione della Direttiva sulle piattaforme (PWD).

In particolare, il Titolo III della direttiva si concentra esclusivamente sul fenomeno della gestione algoritmica del lavoro, introducendo importanti garanzie per la tutela dei lavoratori: l'obbligo di informazione a carico del datore di lavoro/committente; l'obbligo di rendere pubbliche le regole di funzionamento degli algoritmi; il divieto di trattare dati personali sensibili, come indicatori biometrici o lo stato emotivo; la presenza di una supervisione umana nei processi decisionali; e il diritto dei lavoratori di impugnare una decisione algoritmica.

La PWD rappresenta, ad oggi, l'unico atto del diritto dell'UE che affronta in modo esplicito la gestione algoritmica del lavoro, seppure con un ambito di applicazione limitato ai lavoratori impiegati tramite piattaforme digitali. Accanto a essa, tuttavia, si registrano ulteriori iniziative e prese di posizione istituzionali – come, ad esempio, la già menzionata Risoluzione del Parlamento europeo del 17 dicembre 2025[16] – che esercitano una crescente pressione verso un rafforzamento delle tutele in questo ambito.

Il quadro fin qui delineato, sebbene non esaustivo, offre una base idonea per sviluppare una riflessione più ampia sulla necessità di riconoscere e sistematizzare diritti specifici dei lavoratori connessi all'impiego degli algoritmi nel contesto lavorativo, diritti che, allo stato attuale risultano frammentati e dispersi in una pluralità di strumenti normativi.

3. La tutela normativa del lavoratore esposto al *management* algoritmico tende di fatto a riorganizzarsi attorno a nuovi "diritti digitali", funzionali a garantire trasparenza sostanziale e responsabilità giuridica delle decisioni automatizzate, segnando il passaggio da una trasparenza

[16] La Risoluzione nel considerando 19, chiede alla Commissione di elaborare e presentare proposte legislative che regolino l'uso di strumenti algoritmici e dell'IA nella gestione del lavoro, superando il quadro normativo esistente limitato alla direttiva PWD e al GDPR.

meramente formale a un modello fondato sull'*accountability* algoritmica quale nuovo principio ordinatore[17].

In questa prospettiva si colloca la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01), che, pur non introducendo diritti del tutto innovativi[18], consolida un quadro valoriale rilevante: in particolare, il paragrafo 5, lett. d) ed e), dedicato a condizioni di lavoro giuste ed eque, impegna le istituzioni a garantire un uso dell'intelligenza artificiale nei luoghi di lavoro trasparente, basato sul rischio e accompagnato da misure preventive idonee ad assicurare ambienti di lavoro sicuri, la sorveglianza umana sulle decisioni rilevanti per i lavoratori e il diritto di questi ultimi a essere informati quando interagiscono con sistemi di IA; il paragrafo 4, lett. d), richiama inoltre il ruolo del *life long learning* per affrontare le trasformazioni indotte dalla digitalizzazione del lavoro.

La nozione di diritti digitali, tuttavia, rimane eterogenea nei diversi ordinamenti: emblematico è il caso spagnolo, dove la *Ley Orgánica* 3/2018 riconosce un ampio catalogo di diritti digitali, inclusi quelli lavoristici (artt. 87-91), quali il diritto alla riservatezza nell'uso dei dispositivi digitali aziendali, i diritti alla disconnessione digitale e alla tutela della privacy rispetto a videosorveglianza, geolocalizzazione e registrazioni, pur senza prevedere espressamente diritti alla trasparenza algoritmica[19].

Nell'ordinamento italiano, invece, i diritti digitali sono prevalentemente declinati come diritti del cittadino – accesso alle tecnologie, identità digitale, servizi pubblici digitali – attraverso il Codice dell'Amministrazione Digitale d.lgs. n. 82/2005, il GDPR (attuato con il d.lgs. n. 101/2018) e il Decreto Semplificazioni, d.l. 76/2020, lasciando

[17] Per una definizione esaustiva e precisa dell'*accountability* algoritmica v. C. Novelli - M. Taddeo - L. Floridi, *Accountability in artificial intelligence: what it is and how it works*, in *AI & Society*, 2024, n. 39, p. 1871 ss.

[18] L. Cianci, *Dichiarazione europea sui diritti e i principi digitali: quid pluris?*, in *Diritto pubblico comparato e europeo*, 2 aprile-giugno 2022, p. 381 ss. mette in evidenza il carattere superfluo di una dichiarazione *ad hoc* per i diritti già ampiamente riconosciuti a livello normativo.

[19] J.C. Giarcia Quinones, *Il nuovo regolamento dei diritti digitali nel diritto del lavoro spagnolo*, in *Rivista italiana di diritto del lavoro*, 2020, n. 3, p. 167 ss.

ancora aperta la sistematizzazione dei diritti digitali specificamente lavoristici.

In tale scenario, il dibattito sull'*algorithmic accountability* – intesa come relazione di responsabilità tra soggetti e non come attribuzione di responsabilità all'algoritmo in sé[20], fondata sull'obbligo di rendere conto (*answerability*), che presuppone il riconoscimento dell'autorità, la possibilità di interrogazione e la limitazione del potere[21] – assume un rilievo centrale, anche alla luce della crescente delega decisionale a sistemi automatizzati e dell'uso diffuso di strumenti di IA nelle scelte individuali[22].

Non a caso, la sopramenzionata Risoluzione europea del dicembre 2025 ribadisce l'esigenza di una chiara attribuzione delle responsabilità di sorveglianza nell'uso dell'IA nei luoghi di lavoro, nel rispetto del principio dell'*human in control*, precisando che il controllo umano deve essere effettivo e non meramente formale, fondato sulla capacità di comprendere, monitorare e correggere sistemi opachi e complessi, da parte di soggetti adeguatamente formati e dotati di reale autorità.

L'*accountability* algoritmica si pone come strumento per perseguire una uguaglianza sostanziale algoritmica, coerente con la portata prescrittiva del principio di eguaglianza, inteso non come mera descrizione della realtà, ma come criterio di giustizia valutativa, in forza del quale gli eguali devono anzitutto essere riconosciuti come tali per poter essere trattati giuridicamente in modo uguale[23].

Solo attraverso l'integrazione, nel tessuto normativo, di diritti idonei a garantire l'*answerability* dei soggetti responsabili sul concreto funzionamento degli algoritmi è possibile contrastare efficacemente l'opacità e il potenziale discriminatorio dei sistemi algoritmici.

[20] J. Kroll, *Accountability in Computer Systems*, in F. Pasquale - M. Dubber - S. Das, *Eds Oxford Handbook of the Ethics of AI*, Oxford University Press, 2020.

[21] C. Novelli - M. Taddeo - L. Floridi, *Accountability in artificial intelligence: what it is and how it works*, cit., p. 1881.

[22] M. Martorana, *L'"istinto artificiale", come l'AI entra nelle nostre decisioni e cosa implica per il diritto*, 11 dicembre 2025, disponibile online: *https://www.altalex.com/documents/news/2025/12/11/istinto-artificiale-ai-entra-nostre-decisioni-cosa-implica-diritto*.

[23] R. Voza, *Eguaglianza e discriminazioni nel diritto del lavoro. Un profilo teorico*. Relazione AIDLaSS – XXI Congresso nazionale Messina, 23-25 maggio 2024, disponibile online: *https://aidlass.it/wp-content/uploads/2024/05/Relazione-VOZA.pdf*.

In tale prospettiva, il riordino e il coordinamento sistemico – ovvero, ove serve, il riconoscimento esplicito – di un nucleo di diritti digitali dei lavoratori, e in particolare dei diritti alla trasparenza e al controllo delle decisioni algoritmiche, appare come un passaggio necessario per rendere effettiva la tutela contro le diseguaglianze prodotte o amplificate dai sistemi automatizzati.

3.1 Le norme sulla trasparenza consentono al lavoratore – potenziale vittima di discriminazione – di ottenere, prima di un eventuale giudizio, informazioni sul funzionamento dell'algoritmo. Tali informazioni permettono di acquisire una prima conoscenza della possibile discriminazione algoritmica subita.

Le disposizioni del GDPR in materia di informazione e accesso relative ai processi decisionali automatizzati (artt. 13 co. 2 lett. f, 14 co. 2 lett. g e 15 co. lett. h) si applicano a tutte le persone fisiche i cui dati personali sono oggetto di trattamento, indipendentemente dalla natura del loro rapporto di lavoro.

Pertanto, sia i lavoratori subordinati sia quelli autonomi sono titolari di tali diritti, purché i loro dati siano trattati per finalità che incidono sull'accesso al lavoro, sulla gestione del rapporto o sulla cessazione dello stesso. I soggetti obbligati al rispetto di questi diritti sono i titolari del trattamento dei dati personali, ossia le persone fisiche o giuridiche (come le piattaforme digitali o i datori di lavoro) che determinano le finalità e i mezzi del trattamento, nonché i responsabili del trattamento che agiscono per conto del titolare. In pratica, ciò significa che i datori di lavoro e committenti – quando utilizzano algoritmi per l'assegnazione degli incarichi, la valutazione delle *performance* o la determinazione dei compensi – sono tenuti a informare i lavoratori circa l'esistenza di processi decisionali automatizzati, inclusa la profilazione, la logica sottostante al trattamento e l'importanza e le conseguenze previste per l'interessato.

Nel particolare contesto del lavoro svolto tramite piattaforme digitali, indipendentemente dallo *status* del lavoratore, la direttiva PWD impone l'obbligo di trasparenza nell'uso di sistemi automatizzati o semiautomatizzati di monitoraggio e decisione. Ai sensi dell'art. 9, co. 1, lett. a-c, le

piattaforme devono informare: le persone che svolgono il lavoro; i rappresentanti dei lavoratori; su richiesta, le autorità nazionali competenti. Il diritto all'informazione si estende anche alle procedure di reclutamento e selezione (art. 9, co. 5), garantendo così ai lavoratori una piena comprensione del funzionamento dei sistemi decisionali automatizzati che incidono sulle loro opportunità professionali e condizioni di lavoro.

Il valore aggiunto della direttiva PWD – rispetto agli obblighi previsti dal GDPR – consiste nell'obbligo informativo verso i rappresentanti dei lavoratori. Lo sdoppiamento dell'obbligo è giustificabile dalla necessità di evitare l'*overload* informativo, come conseguenza del formale adempimento dell'obbligo legale che veicola le comunicazioni prive di senso per i loro destinatari[24]. Il diritto del lavoro, nella sua elaborazione teorica e normativa, ha storicamente evidenziato che le asimmetrie di potere insite nei rapporti di lavoro non sono superabili mediante il solo rafforzamento informativo del singolo lavoratore, ma richiedono meccanismi collettivi di partecipazione, rappresentanza e negoziazione[25]. I soggetti collettivi da sempre rappresentano interlocutori più idonei a comprendere il senso di dati aggregati e tecnicamente complessi. Solo gli organismi collettivi dotati di rappresentatività dei lavoratori hanno la posizione strategica per lo studio e comprensione del fenomeno, sia addestrando al loro interno i sindacalisti-esperti o comunque rivolgendosi ai professionisti esterni[26].

In Italia, l'art. 1-*bis* del d.lgs. 26 maggio 1997, n. 152, introdotto dall'art. 4 del già richiamato d.lgs. 27 giugno 2022, n. 104 (c.d. Decreto Trasparenza), stabilisce obblighi informativi destinati ai datori di lavoro e ai committenti[27] che utilizzano sistemi decisionali e di moni-

[24] J. Adams-Prassl – H. Abraha, A. Kelly-Lyth - M. 'Six' Silberman – S. Rakshita, *Regulating algorithmic management: a blueprint*, in *European labour law journal*, 2023, vol. 14, n. 3, p. 12 ss.

[25] A. Ingrao, *AI at Work: Reframing Data Protection through the Lens of Labor Law*, in *Diritti lavori mercati*, Int., 2025, n. 1, p. 118.

[26] L. Cini - V. Maccarrone - A. Tassinari, *With or without U(nions)? Understanding the diversity of gig workers' organizing practices in Italy and the UK*, in *European Journal of Industrial Relations*, 2022, vol. 28, n. 3, p. 353.

[27] Per quanto riguarda i soggetti attivi dell'obbligazione, la norma menziona il datore di lavoro e il committente, risultando pacifica l'inclusione dei committenti del lavoro coordinato e continuativo e del lavoro etero-organizzato *ex* art. 2 d. lgs. n. 81/2015.

toraggio automatizzati per concludere, dirigere o controllare contratti e rapporti di lavoro. Il comma 1 specifica che tali obblighi sorgono quando il datore di lavoro o il committente impiega sistemi automatizzati volti a fornire: a) informazioni rilevanti ai fini dell'assunzione o della gestione dei rapporti di lavoro (ad es. attribuzione degli incarichi, trasferimenti, ecc.); b) indicazioni incidenti in materia di sorveglianza e controllo dei lavoratori.

L'art. 1-*bis* attribuisce ai lavoratori – e alle loro rappresentanze – un diritto all'informazione sull'impiego e sul funzionamento dei sistemi decisionali o di monitoraggio automatizzati che incidono sull'organizzazione del lavoro, sulle condizioni di impiego e sulla gestione del rapporto (co. 6, primo e secondo periodo).

L'ordinanza n. 14491 del 3 aprile 2023 del Tribunale di Palermo ha confermato tale interpretazione, chiarendo che il nodo della trasparenza non riguarda tanto l'algoritmo in sé – la cui opacità costituisce un tratto strutturale – quanto i soggetti che lo utilizzano per la gestione dei lavoratori. Il provvedimento ha infatti qualificato come condotta antisindacale, ai sensi dell'art. 28 della l. n. 300/1970, la mancata comunicazione da parte della società alle organizzazioni sindacali delle informazioni relative all'impiego e al funzionamento dei sistemi automatizzati, così come previsto dall'art. 1-*bis* del d.lgs. n. 152/1997, nella formulazione introdotta dal Decreto Trasparenza[28]. Tale pronuncia rafforza la prospettiva secondo cui il diritto dei lavoratori e delle loro rappresentanze a essere informati costituisce un elemento centrale per l'effettiva tutela nell'ambito del lavoro algoritmico.

3.2 In chiave di *accountability* algoritmica, il considerando 71 GDPR e, secondo dottrina minoritaria e giurisprudenza recente, anche gli artt. 15 e 22 GDPR, riconoscono un diritto alla spiegazione delle decisioni automatizzate, da ultimo sancito anche dall'art. 86 dell'AI Act.

[28] Si consenta il rinvio a E. Lacková, *Opacità degli algoritmi e Decreto Trasparenza: il sindacato fa la sua parte*, in *Rivista italiana di diritto del lavoro*, 2023, n. 3, p. 367 ss.

A differenza del GDPR, nel quale l'esistenza di tale diritto è stata oggetto di dibattito interpretativo[29], e risolta solo da ultimo dalla pronuncia della Corte di giustizia dell'Unione europea nel caso C-203/22, *Dun & Bradstreet Austria*[30], l'articolo 86 del AI Act fornisce una base esplicita per il suo riconoscimento – sebbene con un ambito e una funzione limitati – introducendo un vero e proprio diritto alla spiegazione per gli individui coinvolti in decisioni adottate mediante sistemi di IA ad alto rischio.

Inoltre, con l'obiettivo di evitare sovrapposizioni normative e garantire coerenza con i quadri giuridici preesistenti, in particolare con il GDPR, l'art. 86, co. 3 dell'AI Act chiarisce che il diritto alla spiegazione si applica soltanto laddove non sia già previsto dal diritto dell'Unione[31].

Un diritto alla spiegazione per i lavoratori delle piattaforme (qualsiasi sia il loro *status* giuridico) è, invece, specificamente previsto dall'art. 11, co. 1, della Direttiva PWD prevedendo che, qualora una decisione

[29] La prima menzione dell'ipotetica esistenza del diritto alla spiegazione può essere rintracciata in B. Goodman - S. Flaxman, *EU Regulations on algorithmic decision making and a "right to explanation"*, in *Internet data privacy law*, 2017, vol. 7, n. 4; il dibattito si è basato sull'esperienza del diritto alla spiegazione già esistente nella precedente direttiva europea sulla protezione dei dati, antecedente al GDPR, ossia la Direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. Per il dibattito generale sull'esistenza di tale diritto nel GDPR v. S. Wachter - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *Internet data privacy law*, 2017, vol. 7, n. 2, p. 78.

[30] La CGUE ha chiarito che, in presenza di una decisione individuale interamente automatizzata con effetti giuridici o analogamente significativi, l'interessato ha diritto a ricevere informazioni significative sulla logica utilizzata, sufficienti a consentirgli di esercitare in modo effettivo i propri diritti procedurali, inclusi l'intervento umano, l'espressione del proprio punto di vista e la contestazione della decisione, con implicazioni che travalicano il *credit scoring* e si estendono anche all'ambito lavoristico. A. Ponce del Castillo, *The Right to Meaningful Explanation in Algorithmic Management: Commentary on the CJEU's judgment in Dun & Bradstreet Austria*, Case C-203/22 (November 17, 2025). ETUI Research Paper - Technical Brief 2025.02, Disponibile online: *https://ssrn.com/abstract=5821222*.

[31] M. Kaminski - G. Malgieri, *The right to explanation in the AI Act,* in *U of Colorado Law Legal Studies Research Paper*, 2025, n. 25-9, disponibile online: *https://ssrn.com/abstract=5194301*.

interamente o parzialmente automatizzata incida in modo significativo sulle persone che svolgono lavoro su piattaforma, il lavoratore abbia diritto a ricevere una spiegazione riguardante la decisione individuale adottata. Questa disposizione giuridica riconosce il diritto di ottenere una spiegazione di qualsiasi decisione adottata o supportata da un sistema automatizzato e, a determinate condizioni, il diritto di chiederne la revisione. Qualora siano stati lesi i diritti dei lavoratori, la piattaforma è tenuta a rettificare la decisione e ad adottare misure idonee a prevenire il ripetersi di analoghe violazioni in futuro.

3.3 La supervisione umana è tradizionalmente intesa, da un lato, come strumento idoneo a mitigare discriminazioni ed errori nei sistemi algoritmici e di IA e, dall'altro, come meccanismo di *accountability*, in quanto consente di attribuire la responsabilità del controllo a persone fisiche in un contesto in cui i sistemi automatizzati sono privi di soggettività giuridica[32].

La necessità di un coinvolgimento umano nei processi decisionali algoritmici emerge con chiarezza già dalla normativa europea in materia di protezione dei dati personali, in particolare dall'art. 22 del GDPR, pur nei limiti che caratterizzano tale disposizione (v. *supra*, par. 2).

Rispetto al GDPR, e in coerenza con la più ampia visione europea di un'IA antropocentrica, l'art. 14 dell'AI Act adotta un approccio sensibilmente più esteso, applicandosi a tutti i sistemi di IA ad alto rischio, indipendentemente dal settore, dal contesto o dal ruolo svolto nel flusso decisionale[33]. Il diritto alla supervisione umana è funzionale al perseguimento di una duplice finalità: da un lato, la prevenzione dei rischi per la salute, la sicurezza e i diritti fondamentali, anche attraverso la possibilità di intervenire sugli *output* del sistema e correggerli; dall'altro, obiettivi di più ampio respiro, quali la salvaguardia dell'autonomia decisionale umana e il rafforzamento della fiducia nell'impiego dei si-

[32] A.M. Corrêa - S. Garsia – A. Elbi, *Better together? Human oversight as means to achieve fairness in the European AI Act governance*, in *Cambridge Forum on AI: Law and Governance*, 2025, n. 1.

[33] M. Fink, *Human Oversight under Article 14 of the EU AI Act*, 2025, disponibile online: *https://ssrn.com/abstract=5147196*.

stemi di IA. L'art. 14 dell'AI Act impone ai fornitori di predisporre condizioni tecniche e operative idonee ad assicurare una supervisione effettiva, previsione che si coordina con l'art. 26, par. 2, il quale impone ai *deployer* di individuare personale adeguatamente qualificato, dotato della necessaria autorità, competenza e supporto organizzativo.

Infine, anche la direttiva PWD all'art. 10, co. 3, stabilisce l'obbligo di supervisione umana periodica in caso di rischi elevati di discriminazione derivanti da sistemi automatizzati di monitoraggio e decisione. Inoltre, vi è un avanzamento rispetto all'art. 22 GDPR, poiché l'art. 10 estende la disciplina alle decisioni "prese o supportate" da sistemi ibridi di *algorithmic management*, superando le ambiguità normative e rafforzando la certezza giuridica[34].

Tuttavia, nonostante gli sforzi normativi, è stato efficacemente sottolineato come un coinvolgimento umano eccessivo o meramente formale possa risultare controproducente, conducendo a fenomeni di affaticamento decisionale e di *rubber-stamping*, ossia alla mera ratifica acritica delle raccomandazioni generate dai sistemi di *algorithmic management*[35]. La ricerca interdisciplinare dimostra che gli esseri umani tendono a considerare le spiegazioni algoritmiche come indizi generici dell'affidabilità del sistema, senza un reale ingaggio cognitivo, e tali spiegazioni possono addirittura accrescere la fiducia dell'operatore anche in presenza di malfunzionamenti[36].

In tutti gli atti normativi citati emerge inoltre una chiara interdipendenza funzionale tra la trasparenza e l'esplicabilità dei sistemi e l'efficacia della supervisione umana: nel GDPR, i diritti di informazione, accesso e di spiegazione appaiono strettamente connessi alla possibilità di controllo umano. Poiché tali diritti incidono sulla sostanza della decisione, l'impossibilità di comprendere la logica alla base della specifica decisione automatizzata ridurrebbe tali diritti a meri «contenitori vuo-

[34] S. Rainone - A. Aloisi, *The EU Platform work directive. What's new, what's missing, what's next?*, in *ETUI Policy Brief*, 2024, n. 6, p. 6.

[35] J. Adams-Prassl - H. Abraha - A. Kelly-Lyth - M. Silberman - S. Rakshita, *Regulating Algorithmic Management: a blueprint*, cit., p. 20 ss.

[36] Sui possibili *side-effects* negativi della trasparenza e dell'esplicabilità v. A.M. Corrêa - S. Garsia - A. Elbi, *Better together? Human oversight as means to achieve fairness in the European AI Act governance*, cit.

ti»[37];nell'AI Act il diritto alla supervisione umana va letto in combinato disposto con gli artt. 12 e 13[38] che garantiscono tracciabilità, comprensibilità e strumenti per una supervisione umana efficace dei sistemi di IA. Infine, la PWD inserisce il diritto alla supervisione umana nel Titolo III, che include i diritti legati alla trasparenza algoritmica, nonché i diritti di informazione e consultazione. Ciò non solo costituisce un nucleo di diritti interdipendenti a livello sistemico, ma rafforza anche il quadro di protezione dei dati attraverso misure specificamente calibrate sul contesto lavorativo.

4. Prevedendo diritti e obblighi specifici in tema di trasparenza, il legislatore europeo ha dimostrato che ha carpito l'essenza e le unicità della discriminazione algoritmica nel contesto lavorativo fortemente segnato dall'utilizzo di nuove tecnologie per organizzare e controllare il lavoro. Tali diritti fungono da corredo normativo necessario nell'effettiva applicazione del divieto di discriminazione algoritmica sia nell'ambito di lavoro tramite piattaforme digitali che nell'ambito di tutte le prestazioni *standard* ormai impregnate dall'utilizzo degli algoritmi.

Infatti, sebbene i divieti di discriminazione si applichino in linea generale ai rapporti di lavoro – in senso ampio – inclusi quelli dei lavoratori sulle piattaforme digitali, ciò da solo non garantisce un'effettiva parità di trattamento. La presenza di sistemi algoritmici che costituiscono l'intelaiatura tecnologica fondamentale di tali rapporti rende, invece, necessario un quadro normativo specifico che tuteli i lavoratori contro l'opacità delle decisioni algoritmiche.

A tal fine, come evidenziato dalla Risoluzione del Parlamento europeo del 17 dicembre 2025, è necessario riconoscere un nucleo uni-

[37] M. Brkan, *Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond*, in *Internet journal of law and information technology,* 2019, vol. 27, n. 2, p.107 ss.

[38] L'art. 12 obbliga alla registrazione dei *log*, permettendo di tracciare il funzionamento del sistema e facilitandone così il monitoraggio. L'art. 13 stabilisce che il sistema debba essere progettato in modo da consentire al *deployer* di interpretarne correttamente gli *output* e di utilizzarli in maniera appropriata (co. 1), e che le istruzioni per l'uso messe a disposizione del *deployer* includano dettagli sulle misure di supervisione umana, con particolare riguardo agli strumenti tecnici che agevolano l'interpretazione dei risultati (co. 3, lett. d).

versale dei diritti digitali a supporto della trasparenza algoritmica. Tale Risoluzione chiede alla Commissione di elaborare e presentare proposte legislative che regolino l'uso di strumenti algoritmici e IA nella gestione del lavoro, superando il quadro normativo esistente limitato.

È chiaro come l'emersione dei diritti digitali dei lavoratori e del principio di *accountability* algoritmica si pone come risposta alle limitazioni del paradigma antidiscriminatorio tradizionale, messo in difficoltà dall'insufficienza della prova della discriminazione nelle decisioni automatizzate, nonché dal rischio che la neutralità apparente degli algoritmi conduca a una neutralizzazione della responsabilità datoriale.

LIMITS OF THE USE OF ARTIFICIAL INTELLIGENCE (AI) BY EMPLOYERS IN LABOR RELATIONS

Dan Ţop

1. Artificial intelligence (AI) has begun to become a major transformative factor in labor relations. From the automation of processes to algorithms that participate in decision-making regarding hiring, evaluation and dismissal, the use of intelligent technologies puts pressure on the labor legal system. Technological evolution often exceeds the pace of adaptation of legal norms, which can lead to a decrease in the protection guarantees of both the employer and the employee.

The use of artificial intelligence (AI) by employers in employment relationships[1] to simplify and automate certain processes (e.g. candidate selection, employee performance monitoring) is not new. Given the tendency of certain AI systems to perpetuate discriminatory or harmful practices, it has proven necessary to regulate a higher level of protection, by introducing complex obligations for entities that develop or use AI systems in their activity. Digitalization and the development of programs based on artificial intelligence lead to a redefinition of the notion of "workplace".

In the contemporary environment, digital platforms and systems based on artificial intelligence manage human resources activities, work schedules and employee evaluations. Artificial intelligence is used to analyze performance data, monitor productivity and even make decisions on the promotion or dismissal of employees.

[1] Dan Ţop, *Până când roboţii ne vor înlocui,* Ed. Independent, 2024, p. 34 ss.

The relationship between digital platforms and service providers can be qualified as an employment relationship taking into account: the *intuitu personae* character of the activity performed; the prerogative of the direction and control of digital work platforms; the organisational and disciplinary prerogative of the platform[2].

Regulation (EU) 2024/1689[3] establishes the first legislative framework for the classification and control of AI systems, imposing strict requirements for high-risk applications, including those in the field of human resources.

As Giovanni Ziccardi[4] has pointed out, the proposal for a regulation on a European approach to artificial intelligence was born from a series of actions specifically designed to achieve these objectives, thereby creating the first homogeneous and comprehensive legal framework on artificial intelligence ever developed in such detail. The relationship between artificial intelligence and law is one that each area of the world addresses with heterogeneous approaches, from laissez-faire to centralised regulation. According to the author, the European idea, derived from the work on the Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (hereinafter referred to as: AI Law), is that the next decade will focus on the development of reliable and trustworthy artificial intelligence, conceived as a tool that can bring numerous benefits (better healthcare, safer and greener transport, more efficient production processes, etc.), while protecting fundamental rights, without thereby hindering technological development.

2. Regulation 2024/1689, which establishes harmonised rules[5] on artificial intelligence, adopts a risk-based approach, classifying AI sys-

[2] A.G Vâlcelaru, *Munca pe platformele digitale. Delimitari și clarificări,* Ed. C.H. Beck, 2025, p. 167 ss.

[3] *Jurnalul Oficial al Uniunii Europene*, Seria L, 2024/1689, 12.7.2024, in *http://data.europa.eu/eli/reg/2024/1689/oj.*

[4] G. Ziccardi, *L'intelligenza artificiale e la regolamentazione giuridica: una relazione complessa*, in *Diritto del lavoro e intelligenza artificiale*, edited by M. Biasi, Giuffrè, 2024, p.13 ss.

[5] R. Mureșan, *Inteligența artificială în raporturile de muncă – Amenințare sau instrument util?*, in *www.juridice.ro*, 7 noiembrie 2025.

tems into four risk categories, namely: Unacceptable risk – prohibited AI (e.g. social scoring systems or mass surveillance without consent), High risk – AI used in critical areas, including recruitment, selection and assessment of employees, Limited risk – AI with transparency requirements, e.g. chatbots and Minimal risk – AI without special regulations, used for non-critical purposes.

Article 5 of the Regulation expressly mentions prohibited practices in the field of AI, such as: placing on the market, putting into service or using an AI system that uses subliminal techniques that cannot be consciously perceived by a person or intentionally manipulative or deceptive techniques, with the aim or effect of significantly distorting the behaviour of a person or a group of persons by preventing an appreciable reduction of their ability to make an informed decision; the introduction on the market, putting into operation or use of AI systems for the assessment or classification of individuals or groups of individuals over a certain period of time, based on their social behaviour or known personal or personality characteristics.

Marco Peruzzi[6] provides a complete and in-depth analysis of the labour provisions of the AI Law, in their interconnection with other European regulations in force, such as Regulation 2016/679/EU.

Given the significant impact they can have on careers, livelihoods and workers' rights, some AI systems in the field of employment and workforce management are considered to present a high level of risk: those designed to recruit or select individuals, in particular to place specifically targeted job advertisements, to analyse and filter applications and to assess candidates, as well as those designed to take decisions affecting the terms of employment relationships, to promote and terminate employment-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics, or to monitor and evaluate the performance and behaviour of individuals in such relationships.

By way of exception, these systems will not be considered to present a high risk if they do not present a significant risk of harm to the health,

[6] M. Peruzzi, *Intelligenza artificiale e lavoro: l'impatto dell'AI Act nella ricostruzione del sistema regolativo Ue di tutela*, in *Diritto del lavoro e intelligenza artificiale*, cit., p.115 ss.

safety or fundamental rights of individuals (for example, a system performing a limited procedural task, such as detecting duplicates in a large number of applications). Even in exceptional cases, these systems will always be considered to present a high risk if they create profiles of individuals.

For high-risk systems, which may also include artificial intelligence-based programs used in the recruitment, selection and assessment of employees, the Regulation imposes a series of requirements that must be respected by users to ensure their use in accordance with European law. These requirements include the following[7]: implementation of a risk management system (identification and analysis of the known and reasonably foreseeable risks that the high-risk AI system may present, estimation and assessment of the risks that may arise when the high-risk AI system is used in accordance with its intended purpose, adoption of appropriate and specific risk management measures), careful management of the data obtained, adequate technical documentation on how the system is implemented, transparency and continuous provision of data to the implementers and implicitly to the end user, continuous human supervision.

From 2 February 2025, the regulation prohibits the use of AI systems that manipulate the behavior of individuals in a subliminal or deceptive manner, exploit specific vulnerabilities of the individual, implement social scores that may lead to discrimination or prejudicial treatment outside the initial context of data collection, and use risk assessment to predict criminal behavior based on profiling.

AI systems that create facial recognition databases without a specific purpose, infer emotions in the workplace outside of medical or safety purposes, and classify individuals based on biometric data for discriminatory purposes are also prohibited.

The use of remote biometric identification in real time in public spaces by law enforcement is only allowed in cases of emergency or for specific purposes that are strictly necessary and must be authorized in advance by an independent judicial or administrative authority. The

[7] R. Mureșan, *Inteligența artificială în raporturile de muncă – Amenințare sau instrument util?*, cit.

regulation requires annual reporting and guarantees that all such practices are subject to strict conditions to protect individual rights and freedoms.

3. More and more companies are implementing artificial intelligence-based programs in their current activities. The functions and innovations they bring are useful in any field of activity, with programs being developed that can help automate repetitive tasks, provide customer support, prepare personalized marketing strategies or support recruitment and human resources management.

With the advancement of technology and the acceleration of digitalization, «employers have increasingly resorted to sophisticated tools to monitor employee activity. Digital surveillance in the workplace also brings new challenges in the field of occupational health and safety»[8].

«Work monitoring, understood as obtaining, storing and reporting the results of collected observations, has always been a managerial task. Traditionally, it was carried out by supervisors who, while supervising the work of employees, drew conclusions from their observations and implemented corrective actions. The use of information and communication technologies (ICT) for monitoring the employee and their performance has changed monitoring methods, and the popularization of remote work has increased interest in the search for new monitoring systems that use the full potential of new ICT solutions. New developments in the field of ICT have led to the evolution of intelligent monitoring systems and new solutions in electronic work monitoring based on the Internet of Things and Artificial Intelligence, which allow for almost free monitoring. However, scientific knowledge about them is limited and, above all, so is managerial knowledge about the reception of these tools by employees, while their improper use can cause considerable damage»[9].

[8] D. Țop, *Need for use regulations algorithms at the workplace,* in *Revue Européenne du droit social*, 2024, n. 3 (64), p. 7.

[9] J. Woźniak, *Workplace Monitoring and Technology,* Ed. Routledge, 2023.

Currently, the presence of digital technology in European industry is low[10], however, the data must be contextualized taking into account the fact that we are still in a period of transition, in a hybrid model that combines surviving analog companies with emerging smart companies. Certainly, we are in a socioeconomic context in which globalization and its associated phenomena are increasingly pushing towards an inevitable massive digitalization of reality - and of companies - since a large part of the goods and services produced in today's world are made by increasingly technological multinationals. Furthermore, a clear feedback between digitalization and globalization has been highlighted, since the former «is more profound to the extent that it develops in a scenario of a globalized economy, in the same way that globalization spreads more strongly to the extent that it "develops" in a context of digitalization of the economy»[11].

Today, from a technical point of view, the employer has[12] wide possibilities to control or even spy on employees. An example of employee monitoring is keylogger programs that record the list of all programs used by the employee and the words typed on the computer keyboard. Thus, the employer can reconstruct all messages sent via e-mail, web addresses visited, access data and activity on the sites visited. The program can automatically take screenshots, each time an action is performed, and can transmit them online.

A keylogger can automatically record all activity whenever an employee opens a program, a website, types a word on the keyboard or clicks the mouse. The program cannot be identified by the employee, as it does not appear in the list of installed programs or in the taskbar. This is the type of monitoring that the European Data Protection Regulation seeks to eliminate. But implementing the Data Protection

[10] A. García, *Impactos de la gestión laboral algorítmica en las relaciones colectivas de trabajo,* in *Revista Internacional y Comparada de Relaciones laborales y derecho del empleo*, 2024, n. 1 (12), p.134 ss.

[11] J.M. Moreno Díaz, *La difícil concreción de los derechos colectivos en entornos laborales digitalizados*, in *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, 2022, n. 1, p. 152 ss.

[12] I. Alexe, *Monitorizarea salariaților și GDPR - ce nu au voie să facă angajatorii?*, in *https://legislatiamuncii.manager.ro,* 5 decembrie 2025.

Regulation does not mean that an employer can no longer monitor employees for the legitimate purpose of protecting personal property or confidential information.

Employees cannot act against the legitimate interests of their employers; any act that would affect such interests can still be sanctioned. The European Regulation does not in any way aim to reduce the requirement for the protection of objectives or information – if the employee has an interest in protecting their private information, the employer also has an obligation to protect its confidential information. Sometimes the Regulation itself requires the protection of this information, such as the personal data of the company's customers or other third parties.

In order to apply issues related to employee monitoring in Romanian law, Law no. 190/2018 was adopted, which, in art. 5, regulates the processing of personal data in the context of employment relationships. According to this text, if monitoring systems are used by means of electronic communications and/or by means of video surveillance at the workplace, the processing of employees' personal data, for the purpose of achieving the legitimate interests pursued by the employer, is permitted only if:

– the legitimate interests pursued by the employer are well justified and prevail over the interests or rights and freedoms of the data subjects;

– the employer has carried out mandatory, complete and explicit prior information of the employees;

– the employer has consulted the trade union or, where appropriate, the employees' representatives before introducing the monitoring systems;

– other less intrusive forms and methods for achieving the purpose pursued by the employer have not previously proven their effectiveness; and

– the duration of storage of personal data is proportional to the purpose of processing, but not longer than 30 days, except in situations expressly regulated by law or in duly justified cases.

Millions of workers in the EU, according to a study by the European Agency for Safety and Health at Work[13], are working from home

[13] *https://osha.europa.eu*.

or in another way of working remotely, and companies have multiplied their monitoring efforts. For example, in the case of remote work, the global demand for remote productivity monitoring and measurement software has increased by over 54% since the beginning of the pandemic, with various tools available on the market that allow employers to constantly monitor and track what their employees are doing (how many minutes the mouse is inactive, what keys are pressed, screenshots, etc.). It is important that the information that the user enters into the program and the need for the artificial intelligence-based system to be designed to perform a low-level procedural task, do not have a significant influence on the decision-making process or the intended outcome. In the event that a disciplinary investigation is carried out using AI-based programs, or the termination of an employment relationship is in question, it is important that the task performed by the AI system aims to improve the outcome of a previously completed human activity. Given these characteristics, the AI system only adds an additional layer to a human activity, and therefore presents a low risk[14].

AI-based programs have become an extremely important tool in the field of health and safety at work.

The Framework Directive on Health and Safety at Work also includes[15] the obligation for employers to ensure that the planning and introduction of new technologies are subject to consultation with workers and/or their representatives (Article 6(3)(c) of Directive 391/89/EEC).

According to this regulation, employers «have the obligation to take an interest in new technologies emerging in the workplace, and at the same time to inform workers or their representatives, so as not to endanger their health and safety»[16].

Stefania Marassi[17] highlights, on the one hand, that new technologies can help protect the health and safety of workers (thus falling

[14] R. Mureșan, *Inteligența artificială în raporturile de muncă – Amenințare sau instrument util?*, cit.

[15] M. Biasi, *Introduzione*, in *Diritto del lavoro e intelligenza artificiale*, cit., p. 4.

[16] D. Țop, *Drept social european,* Ed. Zven, 2018, p. 175.

[17] S. Marassi, *Intelligenza artificiale e sicurezza sul lavoro,* in *Diritto del lavoro e intelligenza artificiale*, edited by M. Biasi, cit., p. 207 ss.

within the scope of Article 2087 of the Italian Civil Code) and, on the other hand, that the use of AI systems involves significant risks to the physical and mental health of the workforce, risks whose careful assessment and mitigation by the employer could be effectively supported by the proactive and active contribution of the trade union.

More and more companies are starting to use AI technologies to monitor employee activity. Those operating in high-risk sectors, such as the oil and mining industries, are starting to introduce AI systems integrated with drones and sensors that constantly monitor the working conditions of employees or the level of air quality. In the event of a work accident, automatic data analysis helps rescue teams to act quickly and efficiently.

Companies such as DHL, Shell or IBM have started using programs based on artificial intelligence to investigate work accidents. The programs are used to process large volumes of data related to similar incidents and identify the main causes that led to their occurrence, also having a preventive role for the future.

4. The extensive and intensive introduction of AI algorithms and products «raises persistent and systemic challenges at the level of societies, which are manifested in the EU space by the uneven implementation of the adopted legal provisions in the member states; the absence of specific regulations for algorithms in many sectors, including with regard to migrant and seasonal workers; the lack of transparency of algorithms – the so-called "black boxes" which, unlike the homonym often found in aviation, refer to the opacity of decisions adopted based on AI, not to the data recording equipment, which ensures transparency in the case of investigations; and, perhaps, the most controversial and complicated aspect, namely the exclusion of the human factor from the decision-making process and the difficulty of challenging the decisions thus made. Added to this is the high probability of indirect discrimination through the automated use of predetermined criteria»[18].

[18] C.A. Moarcăș, *Protejarea drepturilor fundamentale ale lucrătorilor în contextul algoritmilor*, in *www.juridice.ro*, 10 noiembrie 2025.

Companies such as Amazon and Zillow demonstrate[19] the consequences of the improper use of artificial intelligence.

Zillow, a company operating in the real estate market, began using an AI algorithm to evaluate and estimate the prices of properties that were to be purchased for the purpose of resale. The algorithm overestimated the prices of some properties, which led to purchases at prices higher than the real market value. In 2021, the company suffered losses of over $ 300 million and laid off approximately 2,000 employees.

Between 2014 and 2018, Amazon developed an AI-based recruitment system that assessed candidates for jobs. The system was trained on historical data that reflected a gender imbalance, favoring male candidates. As a result, the algorithm discriminated against women, penalizing resumes that contained terms such as "women" or came from all-female colleges. As a result, the company was forced to abandon the project in 2018.

Examples of administrative jurisprudence include that in France, where in 2021, the *Commission Nationale de l'informatique et des Libertés* – CNIL, the data protection authority, sanctioned a delivery platform for using an algorithm that assessed performance based on opaque criteria, without the possibility of appeal. The decision was considered a precedent in the regulation of artificial intelligence in the workplace. Another example was recorded in Germany: in January 2024, Amazon was criticized in the European Parliament for using algorithms to evaluate warehouse employees, so that, following public and union pressure, the company introduced human reviews and limited worker supervision. In this case, the precedent set in the same period by the Amazon France Logistique case was also invoked, in which the company was fined 32 million euros by the French Data Protection Authority for using a monitoring system considered "excessively intrusive".

5. In Romania, regulations on the impact of artificial intelligence in employment relations are fragmented and insufficient, requiring coordinated legislative interventions. In a period marked by accelerated digitalization and transformations of employment relations, the use of

[19] R. Mureșan, *Inteligența artificială în raporturile de muncă – Amenințare sau instrument util?*, cit.

artificial intelligence in employment relations may raise alarm bells in terms of data protection, non-discrimination, decision-making responsibility and worker supervision.

Romanian legislation is "in the process of transposing the provisions of EU documents, so that, at present, the protection of workers against algorithms is eminently fragmentary and indirectly regulated by three normative acts"[20]: the Labor Code (Law no. 53/2003); Law no. 190/2018 on measures to implement the GDPR, which sets out a framework for data protection at work, but its application is limited; and the Law on Social Dialogue no. 367/2022. In these conditions, there have been malfunctions in the application of the legal provisions, as demonstrated by the case of Bărbulescu vs. Romania (ECHR, 2017)[21], in which the Court established that monitoring employee communications without prior notice violates art. 8 of the European Convention on Human Rights (right to private life); and the Decision of the High Court of Cassation and Justice no. 179/2020[22], which analyzed the limits of the use of algorithms in relation to the rights of authors and end users in the context of the protection of computer programs and emphasized the need for transparency and balance between innovation and legal protection.

The employer must ensure, in addition to compliance with the provisions of European legislation, compliance with the provisions of the Labor Code regarding the respect of the employee's private life; this monitoring must be proportionate and justified, and from the perspective of Law 190/2018[23], personal data obtained with the help of programs based on artificial intelligence must be processed in a clear, transparent manner and limited to clear purposes.

In order to apply issues related to employee monitoring in Romanian law, Law no. 190/2018 was adopted, which, in art. 5, regulates

[20] C.A. Moarcăş, *Protejarea drepturilor fundamentale ale lucrătorilor în contextul algoritmilor*, in *www.juridice.ro*, cit.

[21] *Bărbulescu v.Romania* [EC]-61496/08, Judgment of 5 September 2017, in *https://hudoc.echr.coe.int/eng?i=001-177333.*

[22] Published in Official Gazette no. 694 of 3 August 2020.

[23] Published in Official Gazette no. 651 of 26 July 2018.

the processing of personal data in the context of employment relationships. According to this text, if monitoring systems are used by means of electronic communications and/or by means of video surveillance at the workplace, the processing of employees' personal data, for the purpose of achieving the legitimate interests pursued by the employer, is permitted only if:

– the legitimate interests pursued by the employer are well justified and prevail over the interests or rights and freedoms of the data subjects;

– the employer has carried out mandatory, complete and explicit prior information of the employees;

– the employer has consulted the trade union or, where appropriate, the employees' representatives before introducing the monitoring systems;

– other less intrusive forms and methods for achieving the purpose pursued by the employer have not previously proven their efficiency; and

– the duration of storage of personal data is proportional to the purpose of processing, but not longer than 30 days, except in situations expressly regulated by law or in duly justified cases.

Employers play a key role in protecting workers' fundamental rights in the context of digitalization and the use of algorithms. It is not only a legal obligation, but also an ethical and strategic responsibility, in line with the emerging stage of corporate responsibility, whose contribution to addressing the theme of this article is both imperative and inevitable. Thus, employers must act as "guardians of professional dignity"[24], ensuring that technology becomes a tool to support respect for it, not a means of abusive control.

Romania is at a turning point: it has the basic legislative instruments, but it must quickly adapt them to the realities of digitalized work. Workers' protection can no longer be thought of in traditional terms, as algorithms, AI and migration require a profound rethinking of the legal framework, with a focus on transparency, fairness and dignity.

[24] C.A. Moarcăș, *Protejarea drepturilor fundamentale ale lucrătorilor în contextul algoritmilor*, in *www.juridice.ro*, cit.

6. While smart technologies can bring increased efficiency and safety, their implementation must be done with caution, human oversight and respect for ethical and legal principles to ensure a balance between innovation and the protection of workers' rights. From the recruitment process to the dismissal of employees or the reorganization of the company, the use of artificial intelligence in the workplace brings both significant benefits and notable risks. A balanced understanding and a prudent approach are essential for the implementation of AI within organizations. It is essential to approach this area responsibly, ensuring transparency and respect for ethical principles. In this way, the benefits of this technology will be fully exploited, transforming challenges into opportunities for smarter and more humane work.

ARTIFICIAL INTELLIGENCE AND LABOR RELATIONS WITH REFERENCE TO THE SPANISH LABOR LAW SYSTEM: TWO REALITIES THAT MUST UNDERSTAND EACH OTHER

Juan Carlos García Quiñones

1. The integration of algorithms, or more generally artificial intelligence, into the current dynamics of labor relations has gradually become an undeniable reality[1]. This observation, however, does not limit its reach to the narrow field of labor law. On the contrary, its expansion is evident, with equal or greater intensity, in many other aspects of life in society, posing a challenge to the various branches of law in devising valid solutions to the numerous questions that arise. In short, a wide range of scenarios in different areas of reality – and therefore affecting different branches of the legal system – has emerged, of which we have only given an indicative sample, which nevertheless share the common characteristic of having contributed to fostering a very intense transformation in those areas where they are projected, which will surely be expanded in the near future, placing the Law in the predicament of offering satisfactory solutions under the pressure of this dizzying evo-

[1] J.R. Mercader Uguina, *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Tirant lo Blanch, 2022, p. 17 ss.

lution. In any case, it is confirmed that surprise, astonishment, improvisation, or initial lack of adaptation are not exclusive characteristics of Labor Law, but rather recognizable in all relevant legal systems. This is consistent with the deliberate pace that the Law requires for the solid development of its provisions. This is especially true when changes are so far-reaching and occur so rapidly, as is generally the case with matters related to artificial intelligence. Moreover, given the clear importance of the issues that interact around it, which far surpasses a more or less circumstantial transformation, the demand for answers to such a phenomenon has gone beyond the legal field, to also enter into considerations of an organizational type[2]; or into others of a more clearly extra-legal nature, such as the theme of dialogue between man and machine[3]; or that appeal to ethics[4]. However, this cannot serve as an excuse to avoid the need to implement tangible solutions to the new uncertainties that have arisen. In other words, the search for philosophical or ethical frameworks – which must necessarily accompany and be present – cannot, however, replace the obligation to address the problems raised through fundamentally legal solutions.

2. Without losing sight of the premises examined, and with a focus on Labor Law, evaluating the effects of the transformation brought about by algorithms – or more broadly, artificial intelligence – in the field of labor relations is equally complex, as evidenced by the considerable interest this evolution has generated in recent times among labor doctrine, the judiciary, and other legal professionals involved in Labor Law[5]. In reality, the issue is not so much that digitalization has become a central focus, but rather that the current treatment of numerous labor institutions cannot be approached in isolation from the technological

[2] M.C. Arruga Segura, *La transformación digital en las relaciones laborales y en la organización del trabajo*, Temas La Ley, Wolters Kluwer, 2020, p. 37 ss.

[3] L. Devillers, *Le dialogue homme-machine*, in *Futuribles*, 2019, n. 433, p. 51 ss.

[4] A. Cortina Orts, Ética *de la inteligencia artificial*, in *Anales de la Real Academia de Ciencias Morales y Políticas*, 2019, vol. 96, p. 379 ss.

[5] H. Álvarez Cuesta, *El impacto de la inteligencia artificial en el trabajo: desafíos y propuestas*, Aranzadi, 2020, p. 17 ss.

factor. This conclusion is fully applicable to algorithms and, by extension, to artificial intelligence.

To cite just a few relevant examples, from the principle of transparency in the automated execution of the employment contract, with those references to blockchain technology and artificial intelligence, analyzing issues such as the smart contract, its application to the employment contract with implications in the field of remuneration, from its connection with the fulfillment of the smart contract by the worker, or from the perspective of the intensive processing of the worker's personal data; the analysis of the decision processes in charge of artificial intelligence under that logic of unpredictable automation; the questions raised by the transparency and control of self-executing employment contracts; the very configuration of smart labor contracts; the implementation of algorithms in the actions of labor administration and Social Security; the emergence of new vulnerable groups as a consequence of technology and the resulting need for their social protection; the impact of new technologies on the labor market and their respective influence on the employment of the future; the focus of digitalization on small and medium-sized enterprises, given the wisdom of analyzing any matters related to labor relations considering the size of the company; the projection of artificial intelligence in the prevention of occupational risks; the possibility of providing care through artificial intelligence; or, from a more general perspective, the study of the new challenges posed by algorithms in the respective fields of Law, technology, and ethics.

In coexistence with other doctrinal positions openly critical of the consequences derived from digitalization, to the point of conceptualizing it as an element of fracturing the labor market; when directly alluding to the automation of inequality, under a conception of the tools of advanced technology as instruments of supervision and punishment of the poor; through a call for the need to protect workers in the digital age, based on the simultaneous concurrence of factors such as technology, subcontracting and the growing precarity of work; by graphically contrasting, from that reference point of artificial intelligence, the expression of "diminished workers" versus that of "augmented orga-

nizations"; with the analysis of the consent of food platform workers in algorithmic management, from a "Foucauldian" perspective, so that all knowledge implies power and all power a specific knowledge, so that any discourse is traversed by inherent power relations, conceiving then the algorithms as a great potential source of power susceptible to unbalancing the scales in favor of the employer, to the detriment of the balance that should govern the labor relationship. These opinions confirm the presence of an unresolved question, depending on the final outcome, considering the link between artificial intelligence and labor relations, based on the fundamental trade-off between risks and expectations of improvement. This requires accepting the premise that the coexistence of work with artificial intelligence is an inevitable reality that must be managed, and whose integration will shape the future of employment. This challenge, with artificial intelligence as a key reference point, will undoubtedly also influence the very definition of the right to employment.

Along these lines, it is equally important to highlight the justified concern among trade unions regarding the accelerated implementation of algorithms – or more generally, artificial intelligence – in the dynamics of labor relations. They are aware of the potential dangers this new reality poses for workers, reinforcing their perpetual status as the weaker party in the employment contract[6]. Indeed, the expressed misgivings are normal and certainly understandable, given the employer's "structural" advantage within the employment contract. Any opportunity for modification related to the management of this relationship could encourage the temptation to perpetuate – and, above all, further intensify – this pre-existing *status quo*. Especially when the phenomenon reaches the level of algorithms within the context of the employment relationship. In short, all the conditions are in place for an uncertain scenario, stemming from a situation where the potential impact of change – driven or simply intensified, depending on the assumptions – by algorithms on fundamental issues directly or indirectly affecting the employment relationship will, in any case, be greater and

[6] UGT, *Las decisiones algorítmicas en las relaciones laborales*, *Servicio de Estudios de la Confederación/Análisis y contextos*, 2021, p. 1 ss.

faster than the improvised legal response, even more so when it comes to anticipating changes or preventing the harm resulting from this profound transformation.

Accepting the premise of the growing influence of algorithms in the current context of labor relations immediately raises the question of how to legally address this new reality, for which different degrees of intensity can be identified. A first interpretation, the most lenient with the current *status quo*, would allow one to argue that the configuration of labor law, as it stands, provides a sufficient basis for interpreting any situations that may arise in practice, even with the significant influence of algorithms – or more generally, artificial intelligence –. This position is surely mistaken, as it is complacent, outdated, and decontextualized, given the prevailing situation. A second option, intermediate in terms of the degree of legal intervention, would advocate for including specific references to algorithms in those institutions where they have acquired a proven influence, alluding, for example, to their establishment as a decisive instrument for corporate decision-making; their use as a personnel selection mechanism; in the realm of managerial authority; or their potential as a control and monitoring tool, to name just a few of the most relevant manifestations that confirm the influence of algorithms on labor relations. Thirdly, as a more groundbreaking option, but not necessarily forced given the widespread implementation of algorithms and their transformative potential, it would consist of promoting regulations for the use of algorithms with a cross-cutting dimension within the legal-labor framework.

Furthermore, in this open debate about the position that the legislator should take to address the heterogeneous problems raised as a consequence of this generalization in the use of algorithms, with reference to labor relations, a new variable to consider must be mentioned, namely the creation of the Spanish Agency for the Supervision of Artificial Intelligence, in order to enable the control of algorithms, which has come to light with Law 28/2022, of December 21, *on the promotion of the ecosystem of emerging companies*, whose Seventh Additional Provision is precisely entitled *Creation of the Spanish Agency for the Supervision of Artificial Intelligence*.

The National Artificial Intelligence Strategy, published in November 2020, is framed within the Digital Spain 2025 strategy, including among its ambitious objectives, due to its specific connection with our object of study, the promotion of the creation of qualified employment by boosting training and education, along with the stimulation of Spanish talent and the attraction of global talent; the incorporation of artificial intelligence as a factor of improvement in productivity, efficiency in Public Administration, as well as an engine of sustainable and inclusive economic growth; the generation of a trustworthy environment for artificial intelligence, both in the technological, regulatory and social impact aspects; or the promotion of the global debate on the technological development of humanistic values (Human-Centered AI), focused on ensuring the well-being of society, creating and participating in forums and outreach activities for the development of an ethical framework that guarantees the individual and collective rights of citizens.

As has been seen, the potential projection of the provisions contained in the Seventh Additional Provision of Law 28/2022, of December 21, *on the promotion of the ecosystem of emerging companies*, far transcends the field of labor relations, from the somewhat "imposed" conception of the legislator when he refers, also among that list of objectives, to the enhancement of inclusive and sustainable artificial intelligence, as a cross-cutting vector to face the great challenges of society, with specific allusions to the reduction of the gender gap[7], the digital divide[8], as well as the support for the ecological transition and territorial structuring.

Regardless of whether the ambitious expectations foreseen by the National Artificial Intelligence Strategy are met -or not-, the mere creation of the Spanish Agency for the Supervision of Artificial Intelli-

[7] S. Rodríguez Gonzàlez, *Brechas de género y transformación digital*, in *Revista de Derecho Social*, 2019, n. 88, p. 199 ss.

[8] J. Martínez Girón, *Sobre la brecha digital generacional de la clase media española. Un análisis perspectivístico de Derecho Comparado, relativo a un colectivo gigante de contribuyentes en riesgo de exclusión social"*, in Aa. Vv., *Digitalización, recuperación y reformas laborales (XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social),* in *Colección Informes y Estudios*, Ministerio de Trabajo y Economía Social, 2022, Serie Empleo, n. 62, p. 321 ss.

gence constitutes *per se* a new variable that must be considered, with the potential to facilitate or complicate, depending on the circumstances, the strictly legal treatment that the growing influence of algorithms in labor relations may deserve in the legal-labor system – since this is the area on which we focus our attention – under that logic of promoting greater interventionism through said administrative body. Pending further developments once its operation is consolidated, although it is premature to venture a value judgment on such an initiative, we understand that the task of preserving the fundamental rights of workers as a precaution against a hypothetical abusive use of algorithms requires, above all, adequate legal treatment within labor regulations, consistent with the preservation of existing references also at the constitutional level, subject to the different alternatives we mentioned in previous paragraphs – or others that may arise – as a premise for its interpretation and subsequent application by the jurisdiction. Therefore, the creation of the Agency, contrary to its intended purpose, could distort the legal system, hindering its proper handling of the matter under analysis. However, we are aware of the risk involved in making such an early judgment, given the need to monitor its progress after implementation.

In short, the issues listed above are clearly interrelated. In the following sections, we develop their study using a systematic approach that analyzes, individually, issues such as the establishment of algorithmic logic as a decision-making tool in business, the use of algorithms as a method for personnel selection, the role of algorithms in the realm of corporate management power, and the application of algorithms as mechanisms for business control and monitoring. All these expressions would support the need for legal regulation of the use of algorithms, considering factors such as the continued validity – and even the strengthening – of fundamental rights in the age of algorithms. This must be done while keeping in mind the essential role that collective bargaining is called upon to play in this new era of technological change (Article 37.1 of the Spanish Constitution in conjunction with Article 28.1). Similarly, a specific section on algorithms and trade secrets should be included, addressing the guarantees of transparency regarding the results of their use.

3. The argument about the growing significance of algorithms in labor relations, increasingly evident, in line with the reasons set out in the previous sections, is then reflected tangibly in concrete applications such as, in order, the establishment of algorithmic logic as a decision-making tool in the company; the use of algorithms as a method of personnel selection; the role of algorithms in the field of business management power; or their application as a business control and monitoring mechanism. These expressions, in any case, form an open list for the future, attesting to the prominence of algorithms – or more generally, artificial intelligence – in the current configuration of companies, their business models – with that appeal to the algorithm's potential role as the "heart of the business" – and the organization and management of labor relations. We will analyze these manifestations individually in the following sections.

3.1 The digital transformation of the production system is now an undeniable reality, already shaping and increasingly likely to shape the future of business. Consequently, everything related to artificial intelligence is presented, and even championed, as a fundamental tool for achieving efficiency and productivity. Based on this premise, the use of algorithms as a decision-making tool is becoming increasingly prevalent in various areas of labor relations[9]. From this perspective, the increasing adoption of algorithms by companies is shifting decisions that previously fell – and still fall – within the purview of "traditional" management toward seemingly objective or neutral decision-making models, devoid of any element of subjectivity, arbitrariness, or corporate discretion. However, such a conclusion may prove highly controversial in practice – if not outright refuted – given the new dangers that arise for workers due to the widespread use of algorithms, as we will attempt to explain throughout this study.

Therefore, the concerns, or more moderately, the caution expressed by unions and labor doctrine are fully justified. This is especially true given the current trend toward the widespread use of algorithms, which

[9] J.R. Mercader Uguina, *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, cit., pp. 81 ss.

is extending into many aspects of employers' organizational autonomy, with a clear expansionist intent. These misgivings and precautions have taken concrete form, albeit with a moderate degree of ambition, in the second section of Article 23 of Law 15/2022, of July 12, *comprehensive for equal treatment and non-discrimination*, as already noted, when it mandates public administrations to, within their competences in the field of algorithms involved in decision-making processes, prioritize transparency in the design and implementation and the ability to interpret the decisions adopted by them.

3.2 Among the areas of labor relations where algorithms are poised to play a more prominent role is recruitment, specifically in relation to the use of artificial intelligence by companies as a personnel selection method. There is always a need to balance the respective variables of accuracy and fairness[10]. In this context, there is an initial interpretation, favorable to the virtuality of algorithmic systems as personnel selection tools, based on their apparent effectiveness in evaluating a large group of people homogeneously by using identical parameters during the process. The use of algorithms would then supposedly prevent arbitrary inequality and discrimination.

From this perspective, the objective would be solely focused on achieving maximum efficiency, in this case related to the selection process, regardless – at least initially – of any subjective personal elements imbued with intuitions or prejudices. Following this logic, when a company adopts this strategy in its personnel selection methods, the hiring decision would then be left to "neutral" software, based on the parameters incorporated into the application and once the required professional profile has been defined in detail, considering various factors such as academic qualifications, years of experience, or professional trajectory, among many others.

However, that initial sense of "neutrality" or "objectivity" in personnel selection processes is clearly conditioned – if not outright contradicted – since the subjective factor does not disappear simply by

[10] S. Desiere, *Using artificial intelligence to classify jobseekers:the accuracy-equity trade-off*, in *Journal of social policy*, 2021, vol. 50, n. 2, p. 367 ss.

subjecting the hiring process to such a protocol. On the contrary, this subjectivity exists, only its presence materializes not in the hiring itself, as the final act of the personnel selection process, but in an earlier phase of designing the professional profile of the desired candidate, thus compromising – or biasing, depending on the case – the final result. This is compounded by the fact that this novel approach used in personnel selection processes, stemming from the new decision-making role given to algorithms, can, contrary to what might be intended, significantly hinder the control of discriminatory elements. It is therefore not surprising that labor doctrine has addressed the risks of discrimination associated with the use of algorithms, specifically in this area of personnel selection[11]. However, the potential link between algorithms and discrimination extends far beyond this specific issue[12].

3.3 Another area where algorithms can have significant implications, still within the context of labor relations, is the exercise of managerial authority by employers. To date, digital platforms are the field where algorithms have seen the most intensive development, allowing individual "suppliers" to directly offer their services to the market. Indeed, the integration of the algorithmic model into the computer system enables the automatic assignment of tasks at any given time to the professional best suited to the client's needs. This automated process would replace a hypothetical discretionary decision by the manager or supervisor to assign a client to a specific professional.

A similar result can also occur when applying algorithms to other issues such as scheduling, managed by software configured under these parameters of objective needs. This can lead to additional dangers for workers, for example, an increase in the unpredictability of working hours, conditioned by business interests and managed through the al-

[11] M. Rodríguez-Piñero Royo, *Acceso al empleo, formación y contratación en el contexto de la digitalización*, in Aa. Vv., *Digitalización, recuperación y reformas laborales (XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social), Colección Informes y Estudios*, Ministerio de Trabajo y Economía Social, 2022, Serie Empleo, n. 62, p. 59 ss.

[12] A. Fernández García, *Trabajo, algoritmos y discriminación*, in Aa. Vv., *Vigilancia y control en el derecho del trabajo digital*, Aranzadi, 2020, p. 505 ss.

gorithmic application, with the aim of "automatically" and as closely as possible adapting the working hours of employees to the volume of work required at any given time.

Furthermore, the progressive expansion of algorithms within the context of labor relations has already led to various judicial pronouncements establishing, in their section on proven facts, the algorithmic functions performed by the platform. In light of all the considerations presented, the purposes for the business use of algorithms can be reduced to three basic categories, as systematized by labor doctrine[13], along with a fourth linked to the automated decision on the termination of the contractual relationship[14], with the result that we present below:

a) The allocation of the specific activity, whereby the algorithmic application assigns jobs to the nearest service provider, is one of the factors to consider, along with the inclusion of other variables that also exert a certain influence on this "automatic" or "automated" allocation decision itself, such as tracking jobs proposed and accepted by the service provider in the past, along with the average evaluation received in all those instances from the users of the services provided. This is a complex phenomenon, as can be seen, with the simultaneous interaction of the various elements listed, which labor doctrine has graphically defined as an auction of services coordinated by the algorithm[15].

b) Pricing is assigned through algorithmic management, with service prices varying according to peak demand, in a dynamic pricing system. The current demand volume is the determining factor influencing the standard rate. Service providers can also use this price reference to decide when to provide services, taking advantage of the algorithm's ability to control supplier pricing.

[13] J.R. Mercader Uguina, *La gestión laboral a través de algoritmos*, in Aa. Vv., *Digitalización, recuperación y reformas laborales (XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social), Colección Informes y Estudios*, Ministerio de Trabajo y Economía Social, 2022, Serie Empleo, n. 62, p. 271 ss.

[14] J.L. Goñi Sein, *Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo*, in *Documentación laboral*, 2019, vol. 2, n. 117, p. 60.

[15] J.R. Mercader Uguina, *Algoritmos y Derecho del Trabajo*, in *Actualidad jurídica uría menéndez*, 2019, n. 52, p. 66.

c) Performance evaluation, resulting from the possibilities offered by algorithmic applications for classifying and assessing customer satisfaction with service delivery. This objective is achieved through the almost universal inclusion of service satisfaction evaluation systems, which are also characterized by their immediacy, as is the case in virtually all platforms. This practice has the potential to be extended to a wide range of business models. All these elements lead to the conclusion that the implementation of algorithms, despite their apparent objectivity, does not in itself eliminate arbitrariness in performance evaluation matters unless other corrective mechanisms are also incorporated to ensure their proper use. This is a circumstance that should be borne in mind, especially since, disciplinary aspects aside, the systems designed for performance and objective evaluation are linked to the establishment of variable compensation systems.

d) Automated decision-making regarding the termination of the contractual relationship, resulting from the "automatic" application of predetermined parameters by algorithms, to the point of conditioning the service provider's continued participation. This is based on factors such as a certain volume of accepted orders or user ratings of the services provided, should the established thresholds not be reached. These elements, individually or collectively, could then lead to the automatic disconnection of workers from the platform.

3.4 The use of algorithms also has clear potential applications within labor relations, particularly in crucial aspects of monitoring and controlling workers through video surveillance systems, telephones, geolocation devices, biometric controls, emails, and internet browsing, etc., which significantly increases the effectiveness of these methods from a business surveillance perspective. This increase, in turn, translates into a potential arise in the risk of abuse by employers, as labor doctrine have pointed out[16]. This is especially true regarding the processing of facial recognition software within biometric data. Secondly, regarding

[16] C. Molina Navarrete, «*Duelo al sol» (digital): ¿un algoritmo controla mi trabajo?*, in *Revista de trabajo y seguridad social del centro de estudios financieros*, *Comentarios, casos prácticos*, 2021, n. 457, p. 5 ss.

employee data collected through wearable smart devices (e.g., smartwatches, etc.) provided by the employer and potentially used to track and record employee activity, both inside and outside the workplace. This latter dimension can pose a specific danger, particularly concerning sensitive data such as employee health information, which is generally prohibited from processing. The risks of abuse in the exercise of employer power to monitor and control work can increase significantly with the use of algorithms, depending on the role these algorithms play in all possible combinations of the data obtained, with tangible consequences regarding a potential invasion of employee privacy.

All of this justifies the concern expressed by unions regarding the implementation and progressive use of algorithms in labor relations. Furthermore, algorithms, as control mechanisms, facilitate precision in their exercise or application, and even the generalization of such control. However, paradoxically, this apparent meticulousness can sometimes become a deceptive tool (displaying faces, choosing a number, etc.). For example, a user of a particular service might arbitrarily press one face or another – or respond with a number – when expressing their level of satisfaction with the service received, without any guarantee that this "mechanical" or unreflective action on the part of the user (choosing a face, pressing a button, stating a number, etc.) truly reflects the quality of the service provided. However, it is also worth remembering that the use of algorithms in some cases, and with due diligence, can be beneficial in certain areas, such as occupational risk prevention, as highlighted by the European Agency for Safety and Health at Work in its report entitled *Prospective study on new and emerging risks to safety and health at work associated with digitalization in 2025*.

The aforementioned Report incorporates frequent references to algorithms, with positive or negative consequences for workers, depending on the case, alluding to issues such as the potential impact on workers suffering from stress as a result of the lack of transparency of the algorithms, especially in the so-called "deep learning algorithms" (a technique that uses a family of algorithms that process information in deep neural networks, where what comes out of one level is introduced into the next); the increasingly intense presence of computer

algorithms within digitized management methods, with the danger for workers of loss of control over the content, pace and planning of work, as well as the way in which it is carried out, with consequences in the form of work stress, health and well-being problems, low productivity, increased sick leave, pressure on performance, anxiety and low self-esteem, in contrast to other possible positive consequences such as the derivation of a more effective supervision of the worker's situation and a better knowledge of the risks in terms of safety and health at work in general; a pressure on performance as a prerequisite for an eventual mismatch between the physical and cognitive capabilities of the workers and the job demands, consistent with the incorporation of integrated continuous improvement algorithms, compelling workers to perform with the same speed and efficiency as the machine, giving rise to a phenomenon called "the digital whip" (new forms of discipline and control established through the use of information and communication technologies, so that workers' schedules are set and monitored by computer, often with an integrated continuous improvement algorithm based on the average time it takes workers to complete certain tasks); the significance that ethics and transparency acquire when the decision-making process is carried out through algorithms, with consequences for the trust and acceptance of these systems by workers, as well as regarding their stress levels and other aspects of their mental health; the influence of algorithms on the increase in the autonomy of workers, favoring more horizontal organizational structures, with fewer middle managers, with the consequent negative impact that this can have in the field of occupational safety and health, along with the negative influence on the mental health of workers resulting from the loss of general social interaction at work; the use that companies can make of algorithms to demonstrate compliance with occupational health and safety regulations, as well as in cases of workplace accidents, in addition to taking advantage of the big data generated by the algorithms for a more accurate assessment of risks and the adoption of effective prevention measures; the deprivation of tasks and the loss of qualification that may result for certain workers as a consequence of the generalization of algorithms in the company, limited to exclusive supervisory functions,

requiring lower levels of knowledge and experience, losing the ability to make their own decisions outside the "automated" action of the algorithm, with the risk of boredom and loss of concentration for the worker; the possibility that automation derived from algorithms will remove humans from dangerous environments, in parallel with the introduction, however, of new risks encouraged particularly by the transparency of the underlying algorithms and human-machine interfaces; the positive influence of artificial intelligence monitoring algorithms, based on work interfaces, in protecting the balance between the professional and private life of the worker, preventing unhealthy work practices; or the benefit that derives for workers from the fact that robots and computer algorithms currently carry out many of the routine and repetitive tasks, even though such a consequence is nevertheless subject to certain conditions linked to the configuration of each company or the inherent content of the work performed.

In any case, the examination of some relevant expressions in the use of algorithms within labor relations does not refute a conclusion that is generically valid for all of them: that their presence, despite their apparent objectivity, does not eliminate the existence of the employer's subjective element regarding decision-making that affects the worker. This component of subjectivity materializes precisely when configuring the guidelines that govern the operation of each algorithm. This conclusion holds true for the various scenarios analyzed, as well as for any other situations where algorithms might play a similar role in the future. Ultimately, as labor doctrine have pointed out, the use of biased criteria in algorithm design can negatively impact workers in areas such as employment opportunities, career advancement, and job security[17]. These arguments fuel the debate on the need for specific legal regulations governing the use of algorithms in the workplace, which we will address in the following section.

4. As mentioned earlier, the examination carried out in the previous sections on the growing significance of algorithms in the current state

[17] J.L. Goñi Sein, *Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo*, cit., p. 65.

of development of labor relations, analyzing individually some of its most relevant manifestations such as the establishment of algorithmic logic as a decision-making instrument in the company, the use of algorithms as a method of personnel selection, the role of algorithms in the field of business management power, or the application of algorithms as business control and monitoring mechanisms, offers sufficient guidelines to raise the debate about the need for specific legal regulation regarding the use of algorithms in the company.

This debate, perhaps to put things in their proper perspective, also fails to question the inherent capacity of Labor Law to regulate the new reality in the way it presents itself. This is despite the fact that the discussion about the crisis of Labor Law is indeed a recurring argument among labor doctrine[18]. This is especially true when the changes that labor regulations address go hand in hand with technological development[19]. This circumstance stimulates contributions to provide legal coverage for these transitional situations, as is the case with platforms[20].

In this context, at first glance one might think that the legal system, with its current configuration, offers a sufficient basis to adequately regulate the transformation taking place in labor relations as a result of the increased use of algorithms, through a reinforced appeal to the function of fundamental rights as guarantors of specific areas of personal freedom; the guidelines emanating from the European strategy on artificial intelligence, together with the provisions derived from the General

[18] M. Rodríguez-Piñero - M. Bravo Ferrer, *La difícil coyuntura del Derecho del Trabajo*, in *Relaciones laborales*, 2011, n. 2, p. 75 ss.

[19] J.R. Mercader Uguina, *El futuro del trabajo en la era de la digitalización y la robótica*, Tirant lo Blanch, 2017, p. 79 ss.; C. Molina Navarrete, *Economía de datos, mercados digitales de empleo y gestión analítica de personas: retos para la transición a una "sociedad del e-trabajo decente"*, in *Revista de trabajo y seguridad social del centro de estudios financieros, Comentarios, casos prácticos*, 2021, n. 459, p. 5 ss.; D. Pérez Del Prado, *El debate europeo sobre el trabajo de plataformas: propuestas para una directiva*, in *Trabajo y derecho*, 2021, n. 77, p. 1 ss.

[20] M.L. Rodríguez Fernández, *Nuevas formas de empleo digital: el trabajo en plataformas. Diez propuestas para su regulación internacional*, in Aa. Vv., *Digitalización, recuperación y reformas laborales (XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social), Colección Informes y Estudios*, Ministerio de Trabajo y Economía Social, 2022, Serie Empleo, n. 62, p. 91 ss.

Data Protection Regulation (GDPR)[21]; or the integrative interpretation that the courts may make regarding the inclusion of algorithms in the regulations of Article 44 of the Workers' Statute, concerning business successions, within the context of the so-called "intangible elements" of the company, in line with what has been pointed out by some labor doctrine[22]. All of this is further complemented by the important role that collective bargaining must play.

However, as an alternative, it could equally be concluded that the transformation brought about by the widespread use of algorithms in labor relations would, in itself, justify the implementation of specific regulations on this matter. This would be done to address, with greater effectiveness and a higher guarantee of success, the new dangers facing workers, as the weaker party in the employment contract compared to the employer. This is especially true considering the insufficient protection currently afforded by the mere existence at the European level of an ethical framework to guide the development of algorithms, setting aside the valuable contribution of the GDPR.

All of this is based on the idea that the protection of natural persons in relation to the processing of personal data constitutes a fundamental right (Article 18.4 of the Spanish Constitution), as do the rights to privacy and equality and to not suffer discrimination (Articles 18.1 and 14 of the Spanish Constitution), whose respect must be guaranteed against possible automated decisions carried out by algorithms with the potential to harm them, and may then require specific guarantees to address the risks inherent in artificial intelligence, as has been established by labor doctrine[23]. In this respect, a good opportunity has perhaps been missed to incorporate, within the regulations on digital labor rights contained in Organic Law 3/2018, of December 5, *on the Protection of Personal Data and the guarantee of digital rights*, a specific provision

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).

[22] J.R. Mercader Uguina, *La gestión laboral a través de algoritmos*, cit., p. 265.

[23] C. Sáez Lara, *Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria*, in *Nueva revista española de derecho del trabajo*, 2020, n. 232, p. 85.

dedicated to this issue. This legal text, as is known, gave rise to the first legal regulation of digital labor rights in our legal system.

Given these precedents, Article 23 of Law 15/2022, of July 12, *on comprehensive equality of treatment and non-discrimination*, entitled *Artificial Intelligence and Equal Treatment and Non-Discrimination*, has materialized, with the moderate content observed, a first initiative by the legislator – positive in any case – to address some of the numerous potential dangers associated with the widespread use of algorithms, or more broadly, artificial intelligence. However, it is not decisive enough to settle the ongoing debate about the need for specific regulations on algorithms.

4.1 As previously noted, managing labor-related issues affecting workers through the use of algorithms, if biased criteria are employed in their configuration, can be openly discriminatory, thus disproving any initial appearance of neutrality. It is therefore not surprising that labor doctrine, aware of the dangers posed by the new technological landscape, have focused on studying the link between fundamental rights and labor relations in light of the influence of the digital factor[24]. This applies both to a more general perspective and to specific aspects such as digital reputation[25]. This sensitivity to the described phenomenon is also evident, with a similar level of attention, in comparative law[26]. This will happen, for example, when the collection of worker data is used to make decisions with legal or significant effects on them, in important matters such as access to employment, their placement in

[24] F. Valdés Dal Ré, *Nuevas tecnologías y derechos fundamentales de los trabajadores*, in *Derecho de las relaciones laborales*, 2019, n. 2, p. 129 ss.; M. Rodríguez-Piñero - M. Bravo Ferrer, *Derechos fundamentales y Derecho del Trabajo en el contexto de la economía digital*, in *Derecho de las relaciones laborales*, 2020, n. 10, p. 1233 ss.

[25] A. Pazos Pérez, *La reputación digital mediante algoritmos y los derechos fundamentales de los trabajadores*, in Aa. Vv., *Vigilancia y control en el derecho del trabajo digital*, Aranzadi, 2020, p. 487 ss.

[26] M.C. Escande-Varniol, *Relaciones laborales y derechos fundamentales en la era digital: una visión desde el derecho francés*, in *Temas laborales*, 2020, n. 155, p. 145 ss.; S. Fernández Sánchez, *Relaciones laborales y derechos fundamentales en la era digital: una visión desde el derecho italiano*, in *Temas laborales,* 2020, n. 155, p. 177 ss.

a particular professional level, or the treatment they receive in terms of salary. In this regard, and specifically related to platforms, age has been highlighted as a clear factor of discrimination, considering the importance given to it in job searches on these platforms. Thus, while generally acknowledging employer discretion in hiring, contrary to what might initially appear, the use of algorithms actually accentuates this discretionary factor in access to employment[27].

Similarly, the potential risk of discrimination stemming from the use of algorithms – or more generally, artificial intelligence – is also a recurring argument, particularly regarding its impact on women[28]. Ultimately, the set of manifestations listed in relation to this potential discrimination caused by the application of algorithms or artificial intelligence is as reprehensible as discrimination carried out solely through human intervention. Consequently, there is an obligation to eliminate any discriminatory bias that may occur both during the data collection phase and during the training and programming of algorithms. It is important to note that corporate responsibility is unquestionable in such cases, with the application of legal and conventional norms prohibiting discrimination and Article 14 of the Spanish Constitution.

This provision is continued later in Organic Law 3/2018, of December 5, *on the Protection of Personal Data and Guarantee of Digital Rights*, when it regulates the «General Obligations of the controller and processor», specifying in its article 28.2 a series of cases where the greatest risks that could occur are listed, alluding to «situations of discrimination» (article 28.2.a); the deprivation of the affected parties of their rights and freedoms or the possible impediment of the exercise of control over their personal data (article 28.2.b); as well as the evaluation of personal aspects of the affected parties in order to create or use their personal profiles, specifically, through the analysis or prediction of aspects related to their performance at work, their economic situation,

[27] C. Sáez Lara, *Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria*, cit., p. 87 s.

[28] H. Álvarez Cuesta, *Discriminación de la mujer en la industria 4.0: cerrando la brecha digital*, in Aa. Vv., *La discriminación de la mujer en el trabajo y las nuevas medidas legales para garantizar la igualdad de trato en el empleo*, Aranzadi, 2020, p. 331 ss.

their health, their preferences or personal interests, their reliability or behavior, their location or their movements (article 28.2.d).

Given these precedents, labor doctrine have also identified some inherent features of discrimination originating from algorithms, alluding firstly to their invisibility, with what this implies regarding their additional potential to frustrate the objectives of anti-discrimination laws, along with their instrumental use to reproduce inequalities on a larger scale; secondly, their contribution to potentially increasing the extent and intensity of the discriminatory effect incorporated into the decision-making process through algorithms; and, thirdly, the technical complexity associated with the configuration of algorithmic systems, with the intervention of multiple technical and human elements[29].

Furthermore, with reference to digital platforms, the application of algorithms can generate risks of dehumanization of the worker who carries out the delivery of the product, with what this implies in terms of undermining the dignity of the person, as a consequence of the operations adopted by the algorithmic system itself, with results contrary to the honor and stability in the employment of the worker, who is also absent from the decision-making process and without the possibility of challenging the decision adopted by the algorithm[30]. The dignity of the worker is reflected in Article 20 of the Workers' Statute, which, in paragraph 3, regulates the employer's right to «adopt the measures deemed most appropriate for monitoring and control to verify the worker's compliance with their work obligations and duties, ensuring due consideration for their dignity in their adoption and application and taking into account, where applicable, the actual capacity of workers with disabilities». This is further complemented by the recognition of human dignity in Article 10.1 of the Spanish Constitution, with its inherent inviolable rights, the free development of personality, and respect for the law and the rights of others, as the foundation of political order and social peace.

[29] C. Sáez Lara, *Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria*, cit., p. 90 ss.

[30] J.L. Goñi Sein, *Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo*, cit., p. 66.

Furthermore, the algorithms used in the field of labor relations can potentially also lead to the surreptitious creation of profiles on the health and private life of the worker, with the consequent violation of his right to personal privacy, guaranteed together with the right to family privacy, the right to honor and to one's own image by article 18.1 of the CE. Appeal to the concept of "decent work" which has also been used in labor doctrine, for example, to interconnect the variables of safety and health, on the one hand, and a digital-robotized society, on the other, is crucial[31]. In this sense, given the widespread use of the expression "decent work," as a consequence of the current consensus regarding the inadequacy of simply referring to "work" as a valid benchmark for guaranteeing minimum standards of workers' rights – given their status as the weaker party in the employment contract – it would be worthwhile to also advocate for the adoption of the expression "decent algorithm". This would highlight the necessary oversight of this evolution in labor institutions, driven by technological factors, from a perspective committed to preserving the protective nature of labor law.

Paradoxically, when there is so much talk about the phenomenon of digitization from very varied perspectives, under an apparent peaceful acceptance of this dizzying race towards technification, a new challenge now emerges spontaneously, which consists precisely in uniting the necessary efforts in the search for that "personalization" of the machine or the technological process in question, promoting – or better, ensuring – the incorporation, within the configuration of artificial intelligence, of some features of "humanizing" bias, with the use of expressions that reveal this intention such as "inclusive" or "responsible"[32]. Given this background, section three of Article 23 of Law 15/2022, of July 12, *on comprehensive measures for equal treatment and non-discrimination*, as has been seen, incorporates a mandate directed jointly to public administrations and companies to promote the use of

[31] M. Salas Porras, *Aportaciones de la seguridad y salud en el trabajo para la implementación global del trabajo decente en la sociedad digital-robotizada*, in *Revista internacional y comparada de relaciones laborales y derecho del empleo*, 2019, vol. 7, n. 4, p. 5 ss.

[32] M.P. Blin - Franchomme, *Le défi d'une IA inclusive et responsable*, in *Droit social*, 2021, n. 2, p. 100 ss.

ethical, reliable, and rights-respecting artificial intelligence, following in particular the recommendations of the European Union in this regard. These provisions, in effect, serve almost as a reminder to comply with existing regulations.

4.2 The social and political control of these transformations fully justifies the need for legislators to assume an active role in regulating the use of algorithms in labor relations. This includes establishing minimum standards to prevent potential misuse, especially – though not exclusively – by employers, thereby safeguarding the worker's position as the weaker party in the employment contract. This also serves as a benchmark for more specific, and perhaps more incisive, treatment through collective bargaining. Furthermore, it has a supranational dimension, as exemplified by the reference to the European Framework Agreement on Digitalization, which underscores the importance of the agreed-upon standard[33].

Ideally, a european-level legal regulation should be implemented, moving beyond the initial phase of adhering to ethical principles and replacing them with a more incisive one that adopts strictly legal and mandatory principles of action, with their subsequent implementation in the various national legal systems of the Member States. Such legal regulation could cover various specific aspects, in line with trade union concerns, by addressing issues such as the inclusion of reliability tests in algorithmic processes, the promotion of gender equality and diversity in algorithm design, the widespread use of audits in algorithmic processes, the involvement of public administrations in studying the consequences of applying algorithms on workers' rights and freedoms, and the creation of an appropriate framework of infringements and sanctions related to the misuse of algorithms when it results in detrimental consequences for workers[34].

In this context, as already mentioned, we must cite Article 23 of Law 15/2022, of July 12, *on comprehensive equality of treatment and*

[33] M. Sepúlveda Gómez, *El Acuerdo Marco Europeo sobre digitalización: el necesario protagonismo de la norma pactada*, in *Temas laborales*, 2021, n. 158, p. 213 ss.

[34] UGT, *Las decisiones algorítmicas en las relaciones laborales*, cit., p. 1 ss.

non-discrimination, entitled *Artificial Intelligence and Automated Decision-Making Mechanisms*". However, its provisions do not reach a sufficient level of ambition to settle the ongoing debate about the need for legal regulation to address the risks associated with the widespread use of algorithms, or more broadly, artificial intelligence. This qualifying praise, however, does not diminish our positive assessment of the legislator's initiative.

5. Collective bargaining is destined to be a fundamental instrument in the new era of constant and accelerated technological change, where the use of algorithms is playing an increasingly prominent role. For its part, Organic Law 3/2018, of December 5, *on the Protection of Personal Data and Guarantee of Digital Rights*, also incorporates in its Article 91 a reference to collective bargaining to «establish additional guarantees of the rights and freedoms related to the processing of workers' personal data and the safeguarding of digital rights in the workplace». This provision may also have significant application and implications regarding the use of algorithms within the context of labor relations. Even with all these precedents, as already noted, it is generally clear that issues related to algorithms have not yet had a significant or widespread presence in collective bargaining. Therefore, while there is consensus on the "what" (the need for collective bargaining to assume an active role in addressing algorithms), establishing clear criteria on the "how" (specifying in each case the treatment that should be given in collective agreements regarding the use of algorithms) will be considerably more difficult and still some time away.

6. The analysis of the significance of algorithms in the current state of labor relations, along with the need to implement legal and/or conventional regulations for their use in this area, also warrants a specific section to analyze the interrelationship between algorithms and trade secrets. Indeed, a company's operating protocol, when based on the use of algorithms, with the dimensions analyzed and any others that may arise in the future, can be key to the company's success, as a result of its investment in development and talent (algorithmic companies). This

can even be seen as a way to assert the role of algorithms as a means of transforming data sources, with a definite impact on reducing costs and increasing revenue.

Given these precedents, and considering the exclusion of algorithms from industrial and intellectual property rights, their legal protection must be sought in Law 1/2019, of February 20, on *Trade Secrets*. For this to apply, it is essential that the information or knowledge in question qualify as secret, defined as that which «is not generally known to, or readily accessible to, persons belonging to the circles in which the type of information or knowledge in question is normally used», as stated in Article 1 of the aforementioned legal text. In short, it follows from the provisions of the transcribed legal norm that the only way to prevent the use of the developed algorithm by unauthorized third parties is to maintain its secrecy.

Therefore, the question then arises of the need for transparency in the use of algorithms, which would entail declaring a duty for companies to disclose them. This could directly conflict with the protection of the algorithm's formula for success, since it would be possible to replicate the algorithm if it were to become known to third parties. An intermediate solution between all these competing interests could be the implementation of mandatory audits, which we have already mentioned in previous sections of this study. This would reconcile the company's interest in not revealing the algorithm's formula, on the one hand, with the guarantee that its results are subject to oversight, thus revealing any illegal behavior, on the other. In this respect it is also important to differentiate between the algorithm, which as some scholars have said can be the heart of the company, and the consequences of its use, as well as the data used for the creation of the algorithm itself, which may include biases, whether gender-based or of other types.

For its part, the agreement on the work of delivery riders, reached by the Government, unions, and employers, has finally been formalized in Law 12/2021, of September 28, which amends the consolidated text of the Workers' Statute Law, approved by Royal Legislative Decree 2/2015, of October 23, to guarantee the labor rights of people dedicated to delivery in the field of digital platforms. Its sole article, under the

heading *Amendment of the consolidated text of the Workers' Statute Law, approved by Royal Legislative Decree 2/2015, of October 23*, provides in its first section the introduction of a new letter d) in article 64.4 of the Workers' Statute, with the following wording: «d) To be informed by the company of the parameters, rules, and instructions on which the algorithms or artificial intelligence systems that affect decision-making that may impact the conditions of employment are based, work, access to and maintenance of employment, including profiling»[35].

Ultimately, this is a fundamental transparency rule, designed to safeguard algorithms and artificial intelligence systems as business assets or tools. It also establishes the duty to disclose information regarding the parameters on which these systems are based when they have a demonstrable impact on working conditions, access to and retention of employment, and the creation of employee profiles. This aims to prevent discriminatory outcomes or violations of workers' rights, as well as opaque or non-transparent business decision-making and the exercise of managerial authority. However, collective bargaining subsequently plays a significant role in implementing this provision within each specific business context.

7. The set of manifestations where there is a relevant presence of the use of algorithms, analyzed individually throughout our study with the path that has been seen, by alluding to subjects such as the establishment of algorithmic logic as an instrument in the decision-making processes by companies, the use of algorithms as a method of personnel selection, the role of algorithms in the field of business management power, together with the application of algorithms as mechanisms of control and surveillance of work and of the people who perform it, offers a revealing sample of the importance that they have acquired in the field of labor relations, as well as their growing significance in the near future.

[35] R. Gómez Gordillo, *Algoritmos y derecho de información de la representación de las personas trabajadoras*, in *Temas laborales*, 2021, n. 158, p. 161 ss.; A. Todolí Signes, *Spanish riders law and the right to be informed about the algorithm*, in *European labour law journal*, 2021, vol. 12, n. 3, p. 399 ss.

Similarly, the examination of these statements confirms a conclusion that is generally valid for all of them: their use, despite its apparent objectivity or neutrality, does not actually eliminate the presence of subjective elements in business decision-making that affects workers. This component of subjectivity materializes precisely when configuring the guidelines that govern the operation of the various algorithms. This conclusion is also applicable to any other areas where algorithms may acquire a significant presence in the future. Furthermore, the very formulas employed in connection with the new decision-making role given to algorithms, as seen in the various expressions examined, considerably hinder the control of any potential discriminatory elements.

Furthermore, the various aspects analyzed clearly justify the concerns expressed by unions regarding the implementation and expansion of algorithms in labor relations. It has been established that the use of biased criteria in algorithm configuration can negatively affect workers in areas such as employment opportunities, career advancement, and job security. Therefore, based on the guidelines provided by the various arguments analyzed, the debate regarding the need for specific legal regulations on the use of algorithms in the workplace is certainly well-founded. In this discussion, we advocated for such regulation, with the aim of safeguarding workers' rights, given the new dangers they face as the weaker party in the employment contract, compared to the employer's inherently superior position. This is especially true in the context of the widespread and increasingly prevalent use of algorithms.

Although, from a constitutional perspective, the protection of natural persons in relation to the processing of personal data constitutes a fundamental right (Article 18.4 of the Spanish Constitution), as do the rights to privacy and equality and to not suffer discrimination (Article 18.1 and 14 of the Spanish Constitution), the respect for which must be guaranteed against possible automated decisions carried out by algorithms with the potential to harm them, and may then require specific guarantees to address the risks inherent in artificial intelligence.

In any case, with regard to the Spanish legal system, a good opportunity has been missed to incorporate a specific provision on artificial intelligence into Organic Law 3/2018, of December 5, *on the Protection*

of Personal Data and the guarantee of digital rights, as the text that incorporates the first legal regulation of digital labor rights in Spain. However, as has been pointed out, the current structure of our constitutional legal system offers important tools to legally neutralize many of the dangers that loom over workers as a consequence of the widespread use of algorithms. Therefore, it is up to fundamental rights, rights of freedom or immunity, in labor relations, with their own content and binding force, to deploy their significant reactive capacity against any potential infringements.

On the other hand, as has also been pointed out, among the specific issues to be regulated regarding algorithms, forming an open list of proposals, there should be room for matters such as the inclusion of reliability tests in algorithmic processes, the promotion of gender equality and diversity in the configuration of algorithms, the generalization of the use of audits in algorithmic processes, the involvement of public administrations in the study of the consequences of the application of algorithms on the rights and freedoms of workers, or the creation of an appropriate framework of infringements and sanctions in relation to the misuse of algorithms when they result in harmful consequences for workers. All of this is further complemented by the important and indispensable role that collective bargaining must play in this same respect, as recognized in numerous documents from international organizations, even though the current result is still insufficient, given that issues related to algorithms have not yet achieved a significant or widespread presence in collective bargaining.

For its part, the significance of algorithms in the field of labor relations must also be analyzed from the perspective of their interaction with trade secrets. In this regard, given the confirmed exclusion of algorithms from industrial and intellectual property rights, their legal protection lies in Law 1/2019, of February 20, *on Trade Secrets*, for which it is essential that the information or knowledge in question be secret. Given these precedents, and considering the need for transparency in the use of algorithms, the legal requirement for companies to disclose them could directly conflict with the protection of the algorithm itself, potentially leading to its disclosure to third parties. In this delicate bal-

ancing act, a middle ground could be the implementation of mandatory audits. This would reconcile the business interest in not revealing the algorithm's formula with ensuring its subjection to oversight to prevent any illegal activity.

In any case, the use of algorithms cannot be automatically associated with harm to workers, as this oversimplifies an equation involving numerous variables, as has been shown, which must be considered to reach any conclusion. What does seem undeniable is the increased potential risk to workers resulting from the wide range of possibilities for misuse by employers that algorithms offer, given the unstoppable advance of technology. Therefore, it is incumbent upon Labor Law to exercise extreme caution to ensure their proper use, respecting the essential balance between the respective positions of worker and employer, as parties to the employment contract, choosing among the various possible solutions. These alternative solutions are precisely where the discussion lies, as we have had occasion to examine throughout our study.

This is a crossroads where, for the reasons discussed, Labor Law cannot and should not remain detached, nor should it adopt a passive stance. On the contrary, it must strive to contribute to shaping a regulatory framework with clear rules for the adequate protection of all interests at stake. Indeed, as has already been stated, appealing to ethical or philosophical references, however appropriate and certainly necessary, cannot, replace the need to confront the challenge through fundamentally legal solutions. Given all these precedents, as analyzed throughout our study, Article 23 of Law 15/2022, of July 12, *on comprehensive equality of treatment and non-discrimination*, entitled *Artificial Intelligence and Automated Decision-Making Mechanisms*, certainly constitutes a first step in the right direction. However, it is up to the legislator to continue persevering in the future, with the stated objective of closing any potential loopholes for impunity that may arise within a context dominated by the widespread use of algorithms, or more generally, artificial intelligence.

MINORI ONLINE TRA OPPORTUNITÀ DIGITALI E RISCHI LAVORATIVI: PROFILI DI TUTELA DELLA SALUTE PSICOFISICA

Gisella Emma Comes

Sommario: 1. Minori *online*. – 2. Tecnologie digitali e inedite opportunità. – 3. I rischi del lavoro digitale. – 4. Osservazioni conclusive.

1. Le ultime generazioni hanno visto avvicendarsi alla velocità della luce *walkman*, *streaming*, telefono fisso e *smartphone* sempre a portata di mano, per approdare a un mondo digitalizzato e in progressivo mutamento. A ciascuna il cambiamento ha imposto una sfida che, forse più che per le precedenti, per la generazione attuale, si configura come un profondo mutamento sociale, culturale e psicologico. Le tecnologie digitali sono divenute parte integrante della vita di bambine, bambini e adolescenti; costituiscono strumenti difficilmente trascurabili di comunicazione, relazione e apprendimento. In quanto tali, soddisfano bisogni fondamentali, offrono opportunità di crescita e partecipazione e possono assicurare ai minori il godimento dei propri diritti, sanciti dalla Convenzione ONU sui Diritti dell'infanzia e dell'adolescenza[1].

La pandemia legata alla diffusione del Sars-Cov-2 ha fatto sì che l'impiego della strumentazione tecnologica divenisse sempre più diffuso e ha determinato un abbassamento dell'età d'accesso al mondo digitale. Ciò ha suscitato, dunque, la doverosa attenzione per un fenomeno multiforme e variegatamente sfaccettato, «fotografia delle luci e delle ombre che i ragazzi stanno affrontando nel percorso lungo

[1] *Convention on the Rights of the Child - CRC*, approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989 e ratificata dall'Italia il 27 maggio 1991 con la Legge n. 176.

le autostrade digitali»[2]. La tecnologia, infatti, plasma la società e le relazioni umane[3].

Nell'epoca della rivoluzione dell'*onlife*, di una vita spesa tra reale e virtuale, per sentirsi parte del gruppo, sono indispensabili gli oggetti della connessione e, tra questi, figura, immancabile, lo *smartphone*, custode di legami, segreti, divertimenti di giovanissimi che vivono costantemente connessi.

Rispetto a un'ondata trasformativa che vede impreparata la categoria genitoriale, si alternano approcci "apocalittici", secondo cui internet e i *social media* si caratterizzano per un'elevata pericolosità, a visioni più rosee, secondo le quali il mondo digitale è foriero di inedite opportunità per le nuove generazioni.

Accade, in sostanza, che i genitori stessi finiscano per lasciare i minori liberi di usare le nuove tecnologie perché naturalmente portati a farlo, pur se privi delle necessarie competenze in tal senso, e, in taluni casi, che ne rendano l'esistenza pubblica finanche prima ancora della nascita[4], creando loro delle occasioni favorevoli di varia natura ma anche esponendoli a numerose e significative criticità.

2. Le tecnologie digitali sono fonte di innumerevoli opportunità: indubbiamente facilitano l'accesso alle informazioni, ai dati e alla cultura. Contribuiscono a migliorare le abilità cognitive del bambino e, contestualmente, presentano il pregio di annullare le distanze e i confini, con-

[2] Save the Children, *XIV Atlante dell'infanzia (a rischio) in Italia 2023 – Tempi digitali*, consultabile al link *https://s3-www.savethechildren.it/public/allegati/xiv-atlante-dellinfanzia-rischio-tempi-digitali.pdf* .

[3] Sul tema, si v. A. Sgorlon, *Relazioni connesse: Come essere felici nell'era digitale*, *Centro di formazione e salute digitale*, *Introduzione*, *youcanprint*, 2024; L. Denicolai, *Mediantropi. Introduzione alla quotidianità dell'uomo tecnologico*, Franco Angeli, 2018, p. 156.

[4] Sul punto, si v. A. Lavorgna - M. Tartari, *La sovraesposizione digitale dei minori. Un approccio multidimensionale al fenomeno dello sharenting*, Franco Angeli, 2023, p. 9; L. Aulino, *Tutela dei minori e servizi digitali: i rischi dello sharenting*, in *Familia*, 2022, p. 35 ss.; E. Morotti, *Il dissenso del minore alla pubblicazione delle proprie immagini in rete*, in *Familia*, 2023, p. 1 ss. Il Garante della privacy, con provvedimento n. 681 del 13 novembre 2024, consultabile all'indirizzo *garanteprivacy.it*, ha riconosciuto che la pubblicazione della foto di un minore di 14 anni senza il consenso di entrambi i genitori costituisce un trattamento illecito di dati personali.

sentendogli di coltivare relazioni con amici e familiari fisicamente distanti. Possono costituire fonti di supporto per la crescita del minore.

Se si immagina la realizzazione di un digitale adatto ai più piccoli, diviene immediatamente chiaro che un novero di opportunità afferiscono all'istruzione. La scuola mette a nudo le potenzialità, oltre naturalmente ai *deficit*, del digitale. Se la scuola ha il compito di mettere in campo tutti gli strumenti disponibili per facilitare la partecipazione degli studenti alla vita scolastica[5], le tecnologie di ultima generazione possono rendere l'apprendimento più coinvolgente e personalizzato, offrire mezzi compensativi a chi presenta difficoltà o neuro-divergenze.

Ancora, quali forme di mediazione tra persona e ambiente, possono fronteggiare fenomeni di micro-esclusione degli studenti con disabilità dal contesto scolastico[6], assumendo una funzione di natura compensativa/abilitante, idonea a fungere da supporto concreto nel superamento di difficoltà fisiche e/o sensoriali, oltre che nel renderne effettiva la partecipazione a percorsi di apprendimento[7]. Se usate con consapevolezza, possono divenire una leva di inclusione, riducendo le barriere mediante l'adattamento di contenuti e metodologie ai bisogni degli studenti, unitamente alla previsione di percorsi educativi e di supporto agli insegnanti, che siano da incentivo al dialogo intergenerazionale[8].

[5] Cfr. il decreto legislativo n. 297/1994, *Testo Unico delle disposizioni legislative in materia di istruzione*, e il D.p.r. n. 567/1996.

[6] D. Ianes - H. Demo, *Esserci o non esserci? Meccanismi di push e pull out nella realtà dell'integrazione scolastica italiana*, in *Le Guide*, Erickson, 2015, p.101 ss.

[7] V. Benigno - L. Ferlino - G. Trentin, *Tecnologie abilitanti. Un Nuovo Paradigma per l'inclusione*, in *I quaderni Pearson Academy Serie su Inclusione a 360°. Equità e valorizzazione dei talenti*, Pearson, 2019. Più estesamente, G. Guaraldi, *Ausili, nuove tecnologie e inclusione: alcune esperienze universitarie dalla LIM all'e-learning = Educational aids, new technologies and inclusion: experiences from University Including IWBs and E-learning*, in *L'interazione scolastica e sociale*, 2023, n. 2, p. 34 ss. Cfr. l'indagine condotta da Save the Children, *La didattica inclusiva per bambini con bisogni educativi speciali* in *https://www.savethechildren.it/blog-notizie/la-didattica-inclusiva-bambini-con-bisogni-educativi-speciali.* Anche i soggetti con disturbo dell'apprendimento possono beneficiare dei contenuti fruibili in rete, attraverso l'approccio digitale multimediale, come si legge in Federazione Italiana Medici, *Bambini e adolescenti in un mondo digitale*, Pacini Editore Medicina, 2023, p. 35.

[8] F. Parravicini, *Digitale a misura di minori: tre esempi di innovazione responsabile*, in *https://www.agendadigitale.eu/cultura-digitale/dalla-scuola-alla-sanita-esperienze-concrete-per-educazione-digitale-a-misura-di-bambini-e-ragazzi/*.

Dalla digitalizzazione può derivare, inoltre, un concreto aiuto per i bambini e gli adolescenti che si trovino a fronteggiare complessi percorsi terapeutici, intrisi di paure e ansie: la realtà aumentata e personaggi narrativi possono, in questi casi, rendere i trattamenti terapeutici un'esperienza meno traumatica[9]. Anche mediante il coinvolgimento attivo dei genitori, è supportato il rapporto umano tra medici e piccoli pazienti.

Allo stesso modo, l'esigenza di riconoscere la centralità della persona, accentuata dalla minore età, deve divenire stella polare delle opzioni regolamentari nel caso in cui l'innovazione digitale spalanchi le porte del mondo del lavoro a bambini e adolescenti.

La rete, com'è noto, si è diffusa cavalcando l'idea di un nuovo umanesimo, aperto a un sapere collettivo che, tra l'altro, ne vede interpreti gli utenti *online*. I creativi digitali, anche detti *prosumers* – sintesi e unione dei concetti di *producer* e *consumer* – costituiscono un pubblico produttivo[10]. Si tratta di soggetti che si avvalgono della tecnologia per creare contenuti relativi al proprio modo di essere, ai propri interessi[11], rendendoli accessibili al pubblico che, rispetto ad essi, interagisce avvalendosi dell'uso di una piattaforma.

I veri protagonisti di questo fenomeno sono i primi *digitarian*, ossia coloro che, etichettati come *Generazione Z*, sono accomunati dall'essere i primi nativi digitali[12].

[9] Il riferimento è al progetto *Super Poteri*, realizzato da A. Piras, Ceo di *Brave Potions*, Super Poteri, visionabile al link *https://bravepotions.com/superpoteri/*. L'approccio al paziente è stato oggetto di studio condiviso con psicologi, medici e dentisti affinché risultasse efficace e di semplice utilizzo. Sullo smartphone o il tablet dei genitori, tramite l'*app* Super Poteri, il bambino accede a un mondo fantastico, guidato da due maghi, i cui personaggi hanno i suoi stessi problemi di salute. Dopo il trattamento, il dottore regala al paziente la carta dei poteri. Il risultato è che il lavoro del personale medico risulta agevolato e ottimizzato, la paura dei piccoli pazienti si riduce e, in un ambiente più giocoso, i bambini accettano meglio le cure, come si legge su *https://bravepotions.com/superpoteri/*.

[10] D. Arcidiacono - G. Reale, *Piattaforme e creativi digitali*, in *La giovane Italia*, 2023, n. 4, p. 137 ss.

[11] Per approfondimenti, si v. R. Andò - A. Marinelli, *YouTube Content Creators: volti, formati ed esperienze produttive nel nuovo ecosistema mediale*, Egea, 2017.

[12] Al riguardo, si v. F. Pira, *Figli delle app. Le nuove generazioni digital-popolari e social-dipendenti*, Franco Angeli, 2021.

Per le nuove generazioni, continuamente connesse, si è assottigliata – sino a sparire – la linea di demarcazione tra il naturale andamento della vita quotidiana e il momento performativo digitale, rendendo il primo indistinguibile dal secondo[13] («*performativity is everywhere*»[14]).

Diversamente dal passato, oggi, è mediante i dispositivi mobili che i più giovani dialogano, fanno ricerche *online*, guardano foto, video, *meme*, vedono nascere i primi amori, giocano e lavorano. Bambine/i e adolescenti trovano (o, meglio, cercano) opportunità di guadagno tramite la vendita o lo scambio di contenuti *online* da loro creati e sviluppati.

I cd. *baby influencer* si "alimentano" del numero di visualizzazioni, di *followers* e dei loro commenti, al fine di orientare la propria creatività e preservare il proprio spazio virtuale[15], con la speranza di monetizzare la propria influenza.

Pochi riescono a maturare entrate cospicue, conquistando schiere di seguaci, proprio grazie al supporto dei propri genitori (cd. *family influencer*)[16], fatturando centinaia di euro se non di più, grazie a *social media* che possono rivelarsi una miniera d'oro (*Youtube*, *TikTok* o *Instagram*)[17]. Ma tale fortunata sorte non è per tutti e, anche ove lo sia, *kids* e *baby influencer* finiscono per operare in completa assenza di tutele.

[13] C. Bergonzini, *Nuove frontiere per la tutela dei minori nell'ecosistema digitale: la pratica dello "sharenting"*, in *Quaderni costituzionali*, 2025, n. 2, p. 407 ss.

[14] Espressione di R. Schechner, *Performance Studies: An Introduction*, Routledge, 2013, p. 123.

[15] L. Denicolai - E. Farinacci, *Te lo dico con un video. I linguaggi audiovisivi del quotidiano social*, in *L'avventura*, dicembre 2020, fasc. speciale, p. 145 ss., spec. p. 147; A. Brodesco, *"YouTube come medium generazionale. Figure, pratiche, casi". Schemi, storie e culture del cinema e dei media in Italia*, 2019, vol. 3, n. 6, p. 101 ss.

[16] Per un'analisi del fenomeno, si v. la ricerca *Protagonisti consapevoli? La tutela dei minorenni nell'era dei family influencer*, svolta da *Terre des Hommes Italia* insieme all'Istituto dell'Autodisciplina Pubblicitaria (IAP) e ALMED – Università Cattolica del Sacro Cuore, con il supporto dell'avvocata Marisa Maraffino, consultabile al link *https://terredeshommes.it/pdf/Protagonisti_consapevoli_family_influencer.pdf*, spec. p. 19 ss.

[17] Si pensi, ad esempio, al caso di Nathan Leone Di Vaio, figlio di Mariano Di Vaio, *fashion blogger* tra i più noti e punto di riferimento su internet per la moda maschile, che ha 8 anni, una passione smodata per il golf e 218 mila *follower* su Instagram. O, anche, tra i più conosciuti, negli Stati Uniti, c'è Ryan Kaji, nato nel 2011, ha iniziato a "lavorare" nel 2015, su Youtube ha all'attivo 40 milioni di spettatori e guadagna sui 35 milioni di dollari

3. I rischi più comuni cui il minore può essere esposto sono rappresentati da fenomeni di *data maining*, di *cyberbullismo*[18], di *challenge social*[19], *happy slapping*[20], *denigration* (diffusione di pettegolezzi o di messaggi o materiali offensivi nei confronti delle vittime, con lo scopo di danneggiare la reputazione e le amicizie), *exclusion* (esclusione deliberata di un altro utente da un gruppo *online*, o una *chat*, da un gioco interattivo o da altri ambienti protetti da *password* per provocare nella vittima un sentimento di emarginazione); *exposure* (rivelazione di informazioni private imbarazzanti su un'altra persona); *flaming* (messaggi *online* sottili, violenti, volgari e provocatori intesi a suscitare battaglie verbali in un forum di discussione); *harassment* (invio di messaggi offensivi, volgari o comunque disturbanti attraverso il *web* oppure tramite telefonate mute o dal contenuto sgradevole); *impersonation* (assunzione dell'identità di un'altra persona al fine di spedire messaggi o pubblicare testi offensivi o compiere qualsiasi altra azione lesiva per la vittima a suo

l'anno. Tra le bambine, Anastasia Radzinskaya, youtuber americano-russa, che a 10 anni pare fatturi 100 milioni di euro l'anno; Diana Kydysiuk, assieme alla famiglia porta avanti il *Kids Diana Show*, seguito su Youtube da circa 130 milioni di persone e in continua ascesa; l'australiana Pixie Curtis, a 11 anni, nel 2023, ha deciso di andare in pensione, avendo accumulato, con la sua breve attività di *kid creator* un patrimonio stimato sui 50 milioni di dollari. Al riguardo, cfr. *Baby influencer, guadagni fino a 35 milioni di euro l'anno: e c'è chi a 11 anni va già in "pensione". Ryan, Diana, Anastasia: ecco chi sono,* su *Il Messaggero*, 6 ottobre 2025, consultabile al link *https://www.ilmessaggero.it/economia/schede/baby_influencer_quanto_guadagnano_pensione_11_anni_chi_sono_i_conteggi-5-9109066.html?refresh_ce.*

[18] La Commissione Europea ha presentato un nuovo Piano d'Azione contro il *Cyberbullismo* finalizzato a proteggere la salute mentale di bambini e adolescenti nell'UE. L'iniziativa si articola attorno a tre pilastri: lo sviluppo di una *app* europea per facilitare le richieste di aiuto, il coordinamento degli approcci nazionali e la promozione di pratiche digitali più sicure, reperibile al link *https://digital-strategy.ec.europa.eu/en/library/action-plan-against-cyberbullying*.

[19] Save the Children, *Challenge o sfida social: cos'è e come proteggere i bambini*, reperibile all'indirizzo *https://www.savethechildren.it/blog-notizie/challenge-o-sfida-social-cos-e-come-proteggere-bambini.*

[20] Si tratta del fenomeno della produzione di una registrazione video di un'aggressione fisica nella vita reale a danno di una vittima e relativa pubblicazione online a cui aderiscono altri utenti, che pur non avendo partecipato direttamente all'accaduto, esprimono commenti, insulti e altre affermazioni diffamanti e ingiuriose. I video vengono votati e consigliati come "preferiti" o "divertenti", come si legge sul sito del Ministero della giustizia *https://www.giustizia.it/giustizia/it/mg_2_5_12_1.wp?contentId=GLM1144718*.

nome e/o ottenere informazioni riservate dai suoi amici; *sexting* (invio di messaggi, immagini o video a sfondo sessuale o sessualmente espliciti tramite dispositivi informatici. Si tratta di aggressioni che hanno inizio nella vita reale e continuano con foto o filmati *online*); *outing and trickery* (condotta di chi riceve o detiene dati o immagini intime o dal potenziale diffamatorio della vittima ricevuti direttamente da quest'ultima o, comunque, realizzati con il suo consenso e le pubblica, senza il consenso della vittima o contro il suo espresso dissenso attraverso *chat* e *social network*)[21].

Precisamente, i rischi *online* per i bambini sono stati classificati con quattro C: contenuto, contatto, condotta e contratto. Il bambino può, cioè, essere esposto a contenuti potenzialmente dannosi, ad esempio informazioni o comunicazioni violente o razziste, pornografia, disinformazione, proposte commerciali inappropriate per l'età; può fare l'esperienza di un contatto con un adulto potenzialmente pericoloso rischiando di essere vittima di *stalking*, molestie sessuali, persuasione ideologica; può assistere o essere vittima o partecipare a una condotta potenzialmente pericolosa tra pari d'età; l'eventuale accettazione di condizioni contrattuali può comportare la cessione dei dati del minore, con il connesso rischio di frodi, furto di identità, traffico di immagini pedopornografiche, gioco d'azzardo, persuasione occulta[22]. Né mancano rilevazioni della drammatica diffusione dei fenomeni di tratta e schiavitù di minori a scopo di lavoro forzato e sfruttamento del lavoro (nel mondo, 1 persona su 4 in condizione di sfruttamento o schiavitù moderna è minorenne, pari a 12,3 milioni, dei quali 1,3 milioni sono sottoposti a sfruttamento lavorativo o coinvolti in attività illecite e 320.000 a lavori forzati imposti dalle autorità statali)[23]. E non finisce qui.

[21] Sul punto, v. Federazione Italiana Medici, *Bambini e adolescenti in un mondo digitale*, cit., p. 37 ss.

[22] Cfr. S. Livingstone - M. Stoilova, *The 4Cs: Classifying Online Risk to Children*, in *CO:RE Short Report Series on Key Topics*, 2021; Save the Children, *XIV Atlante dell'infanzia (a rischio) in Italia 2023 – Tempi digitali*, cit., p. 75.

[23] Al riguardo, si v. *Dossier Piccoli Schiavi Invisibili* di *Save the Children*, del 24 luglio 2025, consultabile al link *https://s3-www.savethechildren.it/public/allegati/piccoli-schiavi-invisibili-2025.pdf*.

Giovani e giovanissimi derivano un'idea di sé e della propria personalità dall'immagine proiettata dai *social*[24], esponendosi ai pericoli della rete che si amplificano a dismisura al cospetto dell'innocenza tipica dell'età[25] e assumono peso e concretezza ulteriore quando lo spazio virtuale – abbandonati i connotati ludici – diventa luogo di lavoro, che vede il minore operare in assenza di adeguate previsioni normative di tutela, data anche la facilità di accesso al mercato creativo digitale che rende ostico individuare e arginare forme di sfruttamento del lavoro[26].

Iniziare a lavorare prima dell'età legale consentita determina l'esposizione dei minori a importanti rischi per lo sviluppo e la crescita, non senza effetti sul percorso educativo e sul benessere psicofisico.

Com'è noto, la legge del 17 ottobre 1967, n. 977 tutela il lavoro dei bambini e degli adolescenti poiché soggetti in condizioni di debolezza. Il diritto del lavoro si prefigge di privilegiare l'istruzione, assicurare l'inserimento professionale mediante la formazione, considerando che un'esperienza di lavoro appropriata può contribuire all'obiettivo di preparare i giovani alla vita professionale e sociale da adulti, promuovere il miglioramento dell'ambiente di lavoro per garantire un livello più elevato di protezione della sicurezza e della salute dei lavoratori minorenni, trattandosi di gruppi a rischio particolarmente sensibili[27].

Senza perdere di vista il sistema di tutele che ruota intorno all'interesse superiore del minore – che rispetto a tutti gli altri interessi coinvolti deve assumere una posizione di preminenza[28] – è opportuno evi-

[24] Cfr. A. De Cupis, *I diritti della personalità*, II ed., Giuffrè, 1982, p. 397, il quale teorizza l'identità come sintesi degli elementi che caratterizzano l'individuo; v., altresì, L. Lenti, *L'identità del minorenne*, in *Nuova Giurisprudenza Civile Commentata*, 2006, p. 68 ss.; R. Senigaglia, *L'identità personale del minore di età nel* cyberspazio *tra autodeterminazione e parental control system*, in *Nuova Giurisprudenza Civile Commentata*, 2023, 1568 ss.

[25] M. Giandoriggio, *I minori d'età e i social network: l'insostenibile leggerezza del post,* in *Danno e responsabilità*, 1° maggio 2024, n. 3, p. 296.

[26] C. Di Carluccio, *Digital child labour. Emerging challenges for italian labour law*, in *Revue européenne du droit social*, 2026, n. 1(70), p. 21 ss.

[27] Cfr. Circolare del Ministero del Lavoro e della Previdenza Sociale n. 1 del 5 gennaio 2000.

[28] Il «superiore (o preminente) interesse del minore», proclamato nella Convenzione di New York del 1989 sui diritti del fanciullo (art. 3, par. 1) e rimarcato nella Carta dir. UE

denziare che, a fronte di più o meno reali possibilità di guadagno[29], possono essere compromesse l'identità e l'immagine del minore.

La nuova categoria di lavoratori in parola opera al di fuori del perimetro delle regole e delle tutele, fatta eccezione per le sole ipotesi in cui i soggetti a vario titolo coinvolti nell'espletamento dell'attività (piattaforme, *social network*, *brand*) applichino, di fatto, la disciplina riservata ad altri settori dell'ordinamento (es. diritto d'autore).

Così, numerose e spinose si rivelano le questioni relative alla protezione dei minori che lavorano nel mondo dell'*on line*. I punti di domanda concernono certamente la qualificazione dell'attività svolta[30], la contrattualizzazione del rapporto di lavoro, gli orari di lavoro, la natura e la misura dei compensi[31], le tutele previdenziali[32], e si potrebbe pro-

(art. 24, par. 2), ha assunto portata generale e costituisce «valore apicale di sistema», «nuovo principio sistematico organizzatore di tutto il diritto minorile». Sul punto, si v. V. Scalisi, *Il superiore interesse del minore ovvero il fatto come diritto*, *in Rivista di Diritto Civile*, 2018, p. 407 ss.; E. Lamarque, *Prima i bambini. Il principio dei best interests of the child nella prospettiva costituzionale*, Franco Angeli, 2016.

[29] Sui guadagni realizzati, in generale, dai *content creator*, si v. lo studio *Creator Economy 2025*" realizzato da Kolsquare, società francese specializzata in *influencer marketing,* consultabile al link *https://www.kolsquare.com/en/free-ressources/voices-of-the-creator-economy-by-kolsquare-newtonx?intcmp=skytg24_schede_interlink_text*.

[30] M. Daquino, *Le professioni del lavoro digitale,* in *Web e lavoro. Profili evolutivi e di tutela*, a cura di P. Tullini, Giappichelli, 2017, p. 107 ss.; A. Rota - M. Vitaletti, *La legge francese sugli* influencer*. Quale spazio per il diritto del lavoro?*, in *Labour & Law Issues*, 2023, vol. 9, n. 2, p. C.37 ss.; T. Poell - D. B. Nieborg - B. E. Duffy, *Piattaforme digitali e produzione culturale*, Minimum Fax, 2022; A. Rota, *I creatori di contenuti digitali sono lavoratori?,* in *Labour & Law Issues*, 2021, p. I.1 ss.; D. Mangan, *Influencer markering as labour: between the public and private divide*, in *The Regulation of Social Media Influencers*, a cura di C. Goanta - S. Ranchordas, Edward Elgar Publishing, 2020, p. 185 ss.; P. Iervolino, *Sulla qualificazione del rapporto di lavoro degli influencers*, in *Labour & Law Issues*, 2021, vol. 7, no. 2, p. I.29 ss.

[31] A. Lassandari, *Oltre la "grande dicotomia"? La povertà tra subordinazione e autonomia*, in *Lavoro e diritto*, 2019, p. 96 ss.; A. Alaimo, *Il lavoro autonomo tra nuove debolezze e deficit di protezione sociale: tutele prima, durante e dopo la pandemia*, in *Rivista del diritto della Sicurezza Sociale*, 2021, n. 2, p. 215 ss.

[32] M. D'Onghia, *Lavori in rete e nuove precarietà: come riformare il welfare state?*, in *Quaderni rivista giuridica del lavoro*, 2017, n. 2, p. 83 ss.

seguire a lungo interrogandosi sull'applicabilità degli istituti lavoristici "tradizionali" alle nuove realtà lavorative oggetto di analisi[33].

Sorvolando sulle solo in parte richiamate questioni affrontabili, per ragioni di economia della trattazione, ci si sofferma sui rischi per la salute e il benessere psicofisico del minore, che generano riflessi su di un sano percorso di crescita e di apprendimento e si rivelano potenzialmente idonei a generare povertà ed esclusione sociale del medesimo anche in età adulta[34].

4. Il pericolo insito nell'avanzare del progresso tecnologico è quello di poter rendere non percepibile la lesione dei diritti fondamentali e dei beni giuridici del minore.

A richiamare l'attenzione sulla necessità di ridisegnare ambienti digitali sicuri anche per i bambini, da ultimo, è stata la Commissione europea che ha constatato che il *design* di *TikTok* viola la legge sui servizi digitali, creando forme di dipendenza per l'utente minore di età e adulti vulnerabili. Com'è agevolmente verificabile, il noto *social network*, mediante la perpetua pubblicazione di contenuti, "premia" gli utenti, inducendoli ad avvertire l'urgenza di continuare a *scrollare,* assecondando meccanismi cerebrali che divengono inconsapevoli.

In tal senso, secondo l'indagine europea, la piattaforma non valuta adeguatamente i rischi insiti in detti meccanismi di funzionamento – che agevolmente genera comportamenti compulsivi e riduce l'autocontrollo degli utenti – e ignora, tra l'altro, l'importanza del monitoraggio, a fini anche preventivi, di indicatori quali l'uso compulsivo dell'*app*, il tempo di connessione notturna dei minori, il numero di accessi all'app e altri potenziali indicatori.

Le misure attualmente adottate da *TikTok*, quali gli strumenti di regolamentazione dello *screentime* e i filtri che dovrebbero consentire

[33] Al riguardo, si v. C. Di Carluccio, *Legge 17 ottobre 1967, n. 977 - Tutela del lavoro dei bambini e degli adolescenti. Commento artt. 1-4, 6-8, 15, 17-19, 22-24, 28*, in *Commentario breve alle leggi sul lavoro,* a cura di R. De Luca Tamajo - O. Mazzotta, 2022, p. 923 ss.

[34] C. Di Carluccio, *Non è solo un videogioco! Il lavoro dei pro- players nell'ecosistema degli e-sports*, in *Judicium*, 2024, p. 6.

un effettivo controllo parentale, non sembrano essere adeguatamente efficaci per ridurre i rischi di natura psicosociale derivanti connessi all'utilizzo del *social*. I primi non bastano, nella prassi, a disincentivare né ridurre la dimensione dell'*always on*[35] e i secondi appaiono inefficaci poiché richiedono un impegno specifico dei genitori, sia in termini di tempistiche che di competenze specifiche necessari per attuare il controllo[36].

Assunto a emblema il caso in parola, ampliando il campo d'osservazione, la tutela del minore che lavora nel mondo digitale assume le sembianze di un prisma, dalle numerose sfaccettature, e merita un'attenta riflessione rispetto all'insorgere, in bambini e adolescenti, di patologie e disturbi insiti nell'improprio utilizzo di prodotti e servizi tipici della società dell'informazione[37].

Non esaustivamente, si pensi a stati di irritabilità, perdita del sonno, aumento del peso per scarsa mobilità, insorgenza di comportamenti aggressivi, ansia, depressione, disturbi dell'attenzione[38].

Diviene sempre più sottile la linea di confine tra la realtà *reale* e la parallela realtà *virtuale*, con effetti da evitare, tra i quali la *VR sickness*, ossia malattia da realtà virtuale[39]. La lunga permanenza in una con-

[35] G. Ludovico, *Nuove tecnologie e tutela della salute del lavoratore*, in *Nuove tecnologie e diritto del lavoro. Un'analisi comparata degli ordinamenti italiano, spagnolo e brasiliano*, a cura di G. Ludovico - F. Fita Ortega - T.C. Nahas, Milano University Press, 2021, p. 79 ss.; A. Caracciolo, *Spunti di riflessione sui rischi professionali derivanti dall'iperproduttività autoindotta*, in *Diritto della sicurezza sul lavoro*, 2024, n. 2, p. 250 ss.; C. Di Carluccio, *Quando a stressarsi è l'avatar. Tecnologie immersive e nuove sfide per la tutela della salute e della sicurezza sul lavoro*, *in Ambientediritto.it*, 2024, n. 1, p. 1 ss.; G.E. Comes, *Always on. Tecnostress e benessere nell'ambiente di lavoro*, in *Diritto alla follia. Itinerari storico-giuridici dell'insania*, a cura di C. Saggiomo, C. Scialla, A. Tisci, *Collana I quaderni di Heliopolis*, 11, Aretetra edizioni, 2022, p. 141 ss.

[36] Per approfondimenti, si v. *https://digital-strategy.ec.europa.eu/news/commission-preliminarily-finds-tiktoks-addictivedesign-breach-digital-services-act*.

[37] Per uno studio delle dei vari disturbi connessi all'abuso di internet, si v. Autorità per le garanzie nelle comunicazioni (a cura di), *Libro bianco Media e minori. 2.0. Review*, consultabile sul sito *www.agcom.it.*, p. 15 ss.

[38] Cfr. E.L. Swing - D.A. Gentile - C.A. Anderson - D.A. Walsh, *Television and Video Game Exposure and the Development of Attention Problems*, in *Pediatrics*, 2010, p. 214 ss.

[39] A. Lepore, *Persona, sport e metaverso*, in *Rivista di diritto sportivo*, 2023, n. 2, p. 445.

dizione immersiva può generare disturbi fisici, psicologici, comportamentali e relazionali connessi all'abuso della tecnologia[40].

L'eccessivo utilizzo dei nuovi strumenti di comunicazione digitale e dei videogiochi può generare forme di dipendenza, rispetto alle quali il minore va tutelato[41]. La dipendenza da internet va, infatti, considerata come una vera e propria patologia: nel minore si può manifestare sotto forma di disturbo ossessivo/compulsivo, che induce a un uso eccessivo dello strumento tecnologico e si manifesta mediate l'attuazione di vari comportamenti e in difficoltà di gestione degli impulsi.

Noti sono, ad esempio, la "sindrome di Hikikomori"[42]; la *Fear of missing out*, vale a dire la preoccupazione ossessiva di perdere un evento postato *online*; la *no mobile phone fobia*, ossia la paura di rimanere senza il proprio cellulare che generano stati emotivi negativi, legati a conseguenti comportamenti compulsivi, originanti forme di dipendenza. È intuitivo pensare alla necessità di controllare ripetutamente lo *smartphone*[43].

I prodotti tecnologici sono realizzati per fungere da "specchietto per le allodole", per ipnotizzare l'utente e attirarne in modo crescente l'attenzione, mediante tecniche idonee a cavalcarne eventuali fragilità; per

[40] C. Di Carluccio, *Tecnologie immersive e rischi (vecchi e nuovi) per la salute e la sicurezza del lavoratore. Quali tutele nel metaverso?*, in *Diritto e universi paralleli. I diritti costituzionali nel metaverso*, a cura di A. Fuccillo - V. Nuzzo - M. Rubino De Ritis, Edizioni Scientifiche Italiane, 2023, p. 126. Già nel 2013, l'*American Psychiatric Association* riconobbe la necessità di inserire la dipendenza da videogames o *gaming disorder* tra i disturbi psichiatrici di origine tecnologica, previsti dal Manuale Diagnostico e Statistico dei Disturbi Mentali. Successivamente, nel 2022, l'OMS ha provveduto a classificarla quale malattia mentale nell'*International Classification of Diseases*.

[41] Cfr. T. Cantelmi - C. Del Miglio - A. Gamba, *Contributo allo studio di variabili psicopatologiche correlate all'usoabuso di Internet*, in *Journal of Psychopathology*, 2002, consultabile su *https://www.jpsychopathol.it/article/contributo-allo-studio-di-variabili-psicopatologiche-correlate-alluso-abuso-diinternet/;* T. Cantelmi - M. Talli - S. Putti, *Le nuove frontiere della psicoterapia: il paziente on line*, in *Psicologia contemporanea*, 2000, 160, p. 58 ss.; M. Lucchetta, *La figura dello psicologo: salute e crescita dei pro-player*, in *White paper esports and gaming in Italia 2023*, Osservatorio Italiano Esport, p. 86 ss.

[42] L. Da Re - L. Perulli, *Il ritiro sociale in adolescenza: attualità e prospettive*, Franco Angeli, 2025.

[43] M.D. Griffiths - D.J. Kuss, *Adolescent social media addiction* (revisited), in *Education and health*, 2017, vol. 35, n. 3, p. 49 ss.

orientarne i comportamenti e condizionarne la psiche, con un impatto ancora maggiore in caso di minorenni, com'è intuitivo[44].

Nello specifico caso dei *baby influencer*, le regole imposte dalle piattaforme o dai *brand* (es. frequenza di caricamento dei *post*) – oltre a poter costituire indice di subordinazione, ove lette insieme ad altri elementi caratterizzanti il rapporto di lavoro[45] – possono rappresentare fonte di rischio per la salute del minore.

Fare l'*influencer* e guadagnare solo tramite il lavoro *social* vuol dire, per forza di cose, vivere costantemente connessi, con conseguenze di non poco conto.

Condurre una vita condivisa h24 impone, per avere successo, di interagire continuamente con i *followers*: rispondere ai messaggi, relazionarsi con altri profili, pubblicare contenuti che incrementino questi scambi comunicativi.

Il rovescio della medaglia dell'ambita notorietà è il precario benessere mentale del *creator*, detto anche "stress da *influencer*"[46].

La sovraesposizione digitale dell'*influencer*, che mette la propria vita "in vetrina" e si trova a dover mostrare sempre la migliore versione di sé per non perdere i propri *followers* e agganciarne di nuovi, rende impossibile lavorare secondo orari predeterminati, con l'insorgere di forme di stanchezza solitamente associate a chi esercita attività libero-professionali. Allo stesso modo, il piccolo *influencer* non ha certezze economiche e viva la costante paura di perdere tutto in un istante. Il rischio di *burn out, worhaolism, technostress*[47] e depressione è concreto[48].

[44] I. Garaci, *Il "superiore interesse del minore" nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, in *Nuove leggi civili commentate*, 2021, n. 4, p. 800 ss.

[45] Per approfondimenti, si v. A. Rota, *I creatori di contenuti digitali sono lavoratori?*, in *Labour & Law Issues*, 2021, vol. 7, n. 2, p. I.3 ss.

[46] S. Feldman - S. Almog, *Child work on Platforms. General and Gendered Aspects of YouTubers as Case Study*, in *Labour & Law Issues*, 2024, vol. 10, n. 2, p. 109 ss.

[47] E. Dagnino, *Diritto del lavoro e nuove tecnologie*, Adapt University Press, 2022, spec. p. 85 ss.; V. Pasquarella, *(Iper)digitalizzazione del lavoro e tecnostress lavoro-correlato: la necessità di un approccio multidisciplinare*, in *Argomenti di diritto del lavoro*, 2022, n. 1, p. 50 ss.

[48] A. Castiello D'Antonio, *Malati di lavoro, cos'è e come si manifesta il Workhaolism*, Cooper, 2009, *passim*.

Il minore è esposto, tra l'altro, ai rischi generabili dall'impiego dell'intelligenza artificiale su piattaforme digitali. Infatti, se, da un canto, gli strumenti intelligenti per la salute e la sicurezza, come ad esempio i dispositivi *wearable* o le tecnologie immersive, aprono la strada a innovative forme di prevenzione dei rischi legati alla salute del lavoratore (sensori ambientali, indossabili e sistemi connessi possono infatti raccogliere dati su posture, temperatura, qualità dell'aria e parametri vitali, e consentire, con questa enorme mole di informazioni, di prevedere i rischi, segnalare condizioni critiche in tempo reale e adattare le condizioni di lavoro alle esigenze individuali); dall'altro, il monitoraggio continuo solleva questioni rilevanti in materia di *privacy*, sicurezza dei dati e percezione di controllo da parte dei "mini-lavoratori"[49]. Il pericolo è che i moderni sistemi di IA si trasformino in strumenti di sorveglianza e pressione costante del lavoratore, che ne riducono l'autonomia e ne incrementino lo *stress*[50].

Bambini e adolescenti non sono immuni, poi, certamente ai rischi più propriamente fisici per la salute, quali quelli dei videoterminalisti, anzi tali rischi sono moltiplicati a dismisura, dati gli incessanti tempi di connessione.

4. La previsione di adeguate forme di protezione rispetto ai rischi brevemente elencati, nonché a tutti quelli prevedibili, in adesione

[49] Sul tema v. S. Stefanelli, *Privacy e immagine dei minori in Internet*, in *Cyberspazio e diritto*, 2012, n. 2, p. 233 ss. Come si legge nella comunicazione della Commissione su *Un decennio digitale per bambini e giovani: la nuova strategia europea per un internet migliore per i ragazzi (BIK+)*, COM(2022) 212 final, «oggigiorno i servizi digitali raccolgono e condividono dati sui minori senza soluzione di continuità; la "datificazione" ha inizio persino prima della nascita. Se l'aggregazione di metadati può consentire di ottenere informazioni innovative, ad esempio per quanto concerne la salute e l'istruzione dei minori, la datificazione dell'infanzia può anche provocare ripercussioni potenzialmente negative per tutta la vita sul benessere e lo sviluppo dei minori». Riguardo all'*Internet of Things*, cfr. R. Schulze - D. Staudenmayer, *Digital Revolution: challenges for contract law in practice*, Nomos, 2016, p. 135 ss.; S. Watcher, *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, in *Computer Law & Security Review*, 2018, p. 436 ss.

[50] Al riguardo, *ex multis*, V. Nuzzo, *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, 2018; A. Sartori, *Il controllo tecnologico sui lavoratori*, Giappichelli, 2020.

ai principi lavoristici in materia di salute e sicurezza sul lavoro, presuppone il riconoscimento della subordinazione che ne è condizione d'applicabilità. Il riferimento è alle previsioni di cui all'art. 2087 del codice civile nonché a tutte le misure previste dal Testo Unico in materia di salute e sicurezza sui luoghi di lavoro che impongono, tra l'altro, l'adozione di misure specifiche data la minore età dei soggetti da proteggere (es. redazione del Documento di valutazione dei rischi in base all'età)[51]. Sempre alle stesse condizioni, sarebbero configurabili le tutele indennitarie conseguenti a infortuni o malattie professionali, derivanti dalla stipulazione dell'assicurazione INAIL.

Attualmente, in Italia[52], una normazione *ad hoc* è prevista dalla Proposta di legge n. 1771 del 12 marzo 2024, rubricata *Modifiche alla legge 17 ottobre 1967, n. 977, in materia di impiego dei minori nell'ambito delle piattaforme digitali di condivisione di contenuti multimediali, nonché disposizioni sulla diffusione del l'immagine e di contenuti multimediali di minori*.

Persistendo, però, un vuoto normativo in materia, risulta difficile e comunque incerta l'individuazione della titolarità degli obblighi di tutela del minore, non essendo agevole l'identificazione del soggetto che, a seconda del caso concreto, funga da datore di lavoro.

In attesa della laboriosa trasformazione del progetto di legge in legge, data l'oggettiva difficoltà d'identificazione dei soggetti formalmente responsabili della tutela del minore che di fatto esercita la professione d'*influencer*, non appare imprudente ritenere tali, a seconda del ruolo svolto, tutti coloro che sono coinvolti. Ci si riferisce ai genitori o soggetti esercenti la potestà genitoriale[53], alle piattaforme, ai *brand* eventualmente pubblicizzati, a eventuali associazioni di categoria e sinda-

[51] L. Baraldo - L. Magagnato - A. Faccio, *Metodo ARAI®: nuovo approccio di elaborazione del DVR in riferimento all'età*, in *Igiene e sicurezza sul lavoro*, 2017, n. 7, p. 391 ss.

[52] In Francia vi è già una normazione. In tal senso, si v. la legge 19 ottobre 2020, n. 1266 e la legge del 9 giugno 2023, n. 451.

[53] Come sottolineato dalla Federazione Italiana Medici, *Bambini e adolescenti in un mondo digitale*, cit., p. 3: «Basterebbe una semplice domanda, chiedere ai genitori se mai lascerebbero il proprio figlio in un luogo sconosciuto senza dare consigli per la sua sicurezza».

cati, all'utente finale, ai gestori di servizi pubblicitari, all'Ispettorato nazionale del lavoro.

Sicuramente auspicabile sarebbe l'adozione di misure preventive di ampio respiro, come la previsione di programmi formativi del minore e la disciplina dei tempi di connessione; senza tralasciare forme di monitoraggio del lavoro minorile e di coinvolgimento responsabile anche delle imprese che con il minore si interfacciano, sia pure in modalità virtuale.

L'integrità del benessere pisco-fisico del lavoratore digitale è un valore imprescindibile che trae (e deve trarre) linfa dal sistema normativo lavoristico e assume il valore di un prezioso investimento (anche) per il futuro ove declinato a misura di bambino.

CONSIDERATIONS REGARDING FIXED-TERM INDIVIDUAL EMPLOYMENT CONTRACTS IN THE EUROPEAN UNION

Marius Mihălăchioiu

1. The fixed-term employment contract is a fundamental institution of the European labour market, yet simultaneously one of the most problematic forms from the perspective of social protection. Directive 1999/70/EC explicitly acknowledges the inherent risk of precariousness[1]. At the same time, the CJEU has developed a consolidated doctrine regarding the obligation of Member States to prevent abuses[2].

Professor Antonio Baylos Grau, in his acceptance speech for the title of Doctor Honoris Causa at Valahia University, highlighted two elements that constitute «the coordinates within which labour law operates, beyond its dogmatic configuration. First, the conditioning of this legal system by the economic situation, particularly with regard to the impact that economic crises may have on its constituent elements. Second, the dependence of the organisation of work on technological change». In both cases, his argument sought to summarise what may be regarded as a truism: «that the meaning and function of Labour Law are conditioned by the political decisions that guide it and that, consequently, there is no single way of addressing the challenges that

[1] Directive 1999/70/EC, in Recital (6), states that «whereas open-ended employment contracts are the general form of employment relationships and contribute to the quality of life of the workers concerned and to improving performance».

[2] Case C-212/04, *Adeneler and Others v. Ellinikos Organismos Galaktos* (ELOG).

economic crisis and technological innovation pose to the legal systems of nation-states»[3].

In the same speech, he also highlighted issues related to labour precariousness: «European labour-law scholars have had to confront a key term – an authentic oxymoron – flexicurity: that is, the method devised by the Barroso Commission to 'modernise' European labour law by reducing individual and contractual employment guarantees while simultaneously increasing, in an uneven manner, those derived from social benefits, depending on each country's system of protection. This involved inducing a profound shift in the employment guarantees derived from our social constitutions, which had been based on a precarious balance between the right to work and the freedom to conduct business in a market economy. A century which, for Romania, signified the long-awaited integration into the legal order of the European Union, in what became the sixth enlargement of this economic and political conglomerate – postponed until 1 January 2007 – after which followed the long march toward meeting the economic convergence criteria required by the single currency, the euro, still not completed».

2. Initially, the legal relationship based on a fixed-term employment contract was the subject of a Commission proposal for a Council Directive. The European Parliament delivered its opinion on the proposal on 24 October 1990 (Official Journal C 295, 26.11.1990)[4].

Within the Council, no consensus could be reached, and therefore the Commission decided to proceed with consulting the social partners under Article 3 of the Agreement on Social Policy. During the first consultation, the social partners emphasised the need to combat discrimination against workers affected by new and flexible working conditions. At the end of the second round of consultations, the social partners decided to begin negotiations in this area[5].

[3] Antonio Baylos Grau, Speech on the occasion of receiving the title of Doctor Honoris Causa awarded by Valahia University of Târgoviște, in the brochure *Antonio Baylos Grau – Doctor Honoris Causa*, published by Valahia University of Târgoviște, 2025, p. 39.

[4] *eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990PC0228(01).*

[5] *https://eur-lex.europa.eu/RO/legal-content/summary/fixed-term-work.html.*

On 6 May 1999, the Parliament adopted a resolution on the Commission's proposal, calling on the Council to approve the framework agreement on fixed-term work (not published in the Official Journal). However, the Parliament expressed regret that the agreement covered only successive employment relationships, that the rules designed to prevent abuse through successive fixed-term contracts did not include qualitative or quantitative obligations, and that no measures had been taken to ensure priority access to newly created jobs or to guarantee that such workers would have access to appropriate vocational training[6].

The legal regime applicable to fixed-term employment contracts is established primarily through Directive 1999/70/EC and the CES–UNICE–CEEP Framework Agreement. The objectives of the Directive are:

(a) the prevention of abuses, and

(b) the prohibition of discrimination between workers employed under fixed-term contracts and those employed under open-ended contracts.

3. Atypical employment refers to forms of work that deviate from the standard model, such as part-time contracts, fixed-term contracts, casual work, or platform work[7].

Standing defines precariousness as a combination of contractual instability, economic uncertainty, and a lack of control over working conditions[8].

[6] *https://eur-lex.europa.eu/RO/legal-content/summary/fixed-term-work.html.*

[7] Eurofound, *Future of Work: Employment Structure in Europe*, p. 14 ss., Publications Office of the European Union, 2019.

The European Foundation for the Improvement of Living and Working Conditions (Eurofound) is a tripartite agency of the European Union established in 1975. Its role is to provide knowledge that contributes to the development of better social, labour, and employment policies, in accordance with Regulation (EU) 2019/127, in *https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/eurofound_ro.*

[8] G. Standing, *The Precariat. The new dangerous class*, Bloomsbury Publishing Plc, First published in 2011 Reprinted 2011 (three times), 2012 (three times), 2013, edition first published 2014, p.1.

Serge Paugam is one of the first authors to distinguish between precarious employment and precarious jobs. In Paugam's analysis, precarious employment concerns the vulnerable contractual relationship between employee and employer, whereas precarious jobs reflect the poor or deficient content of the work itself[9].

We will focus on the study and analysis of vulnerability within the contractual employment relationship, without examining the sociological aspects. The legal relationship is characterised by instability, a lack of guarantees, an excessive dependence on the employer, limited prospects for professional development or stability, and a high risk of dismissal[10].

Eurofound confirms that workers employed under fixed-term contracts face the highest risk of precariousness within the EU[11]. The main determining factor is the structural dependence on contract renewal, which reduces their bargaining power.

The main determining factor is the structural dependence on contract renewal, which reduces workers' bargaining power.

The Opinion of the European Economic and Social Committee on *Precarious work and mental health* – 2023/C 228/05[12], referring also to the European Parliament Resolution of 4 July 2017[13], which stated

[9] S. Paugam, *Le salarié de la précarité: Les nouvelles formes de l'intégration professionnelle*, Presses Universitaires de France (PUF), 2007, p. 18 ss. Serge Paugam is an internationally renowned sociologist whose works on inequalities, social segregation, and contemporary forms of social bonds are considered authoritative. His research focuses primarily on the sociology of work.

[10] S. Paugam, *Le salarié de la précarité: Les nouvelles formes de l'intégration professionnelle*, cit.

[11] Eurofound, *Precarious work in Europe*, 2022.

[12] *Official Journal of the European Union C 228/28 of 29 June 2023*, in *https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=uriserv%3AOJ.C_.2023.228.01.0028.01.RON&toc=OJ%3AC%3A2023%3A228%3ATOC.*

[13] In the Official Journal of the European Union, C series 334/2 of 19 September 2018, the European Parliament Resolution of 4 July 2017 on European standards for the 21st century was published, in *https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=uriserv%3AOJ.C_.2018.334.01.0002.01.RON&toc=OJ%3AC%3A2018%3A334%3ATOC*; see also *https://www.juridice.ro/603280/rezolutia-parlamentului-european-din-4-iulie-2017-ref-standardele-europene-pentru-secolul-21.html.*

that precarious work is «a form of employment that does not comply with EU, international or national norms and standards and/or does not provide sufficient means for a decent standard of living or adequate social protection», concluded that work can be a protective factor for mental health but may also contribute to the development of illnesses, which is why the WHO considers it a social determinant of health[14].

The rapporteur highlights the relationship between precariousness and fixed-term individual employment contracts. José Antonio Moreno Díaz[15] states that «forms of precarious work include: involuntary part-time jobs; low wages that do not allow workers to meet basic needs; zero-hour contracts or on-call or temporary contracts used to cover structural needs; constant uncertainty regarding the duration of employment, working hours, pay, tasks, etc.; lack of autonomy and limited opportunities for career progression; excessive demands leading to extended or intensified working time, generating conflict between professional and family life. Such forms of work are rarely a voluntary choice for workers, although there are workers who do choose them»[16].

In the same consultative document, one of the most important conclusions of the study is included under the chapter Specific Observations. The justification for protecting workers employed under fixed-term employment contracts is given by the statement that «the imbalance of power between capital and labour constitutes a risk factor for precarious work. This imbalance must be equalised, both through legislation and through social dialogue and trade union action, creating a context that protects workers while at the same time maintaining favourable economic conditions and avoiding unfair competition»[17].

Even if employment relationships are covered by open-ended individual employment contracts – which continue to represent the general

[14] Point 1.2 of the Opinion of the European Economic and Social Committee on "*Precarious work and mental health*", 2023/C 228/05.

[15] *https://www.openaccessgovernment.org/contributor_profile/jose-antonio-moreno-diaz-eesc-member/*.

[16] Point 1.4 of the Opinion of the European Economic and Social Committee on "*Precarious work and mental health*", 2023/C 228/05.

[17] Point 3.1 of the Opinion of the European Economic and Social Committee on "*Precarious work and mental health*", 2023/C 228/05.

rule in the European Union, as they offer the highest level of legal and social protection – there is nevertheless a counterbalance generated by fixed-term contracts and other forms of atypical employment. Although legitimate and necessary in a dynamic economy, these forms carry a structural risk of precariousness: instability, unpredictable income, reduced bargaining power, and unequal access to social protection and vocational training.

In this entire context, flexicurity was conceived within the European Employment Strategy as a mechanism to prevent precariousness, on the assumption that contractual flexibility must be compensated by robust social protection and universal access to training[18].

However, during the 2009-2011 financial crisis, the Member States implemented only the flexibility component, without the accompanying security measures, and the result was a general increase in precariousness. This phenomenon is documented by Eurofound. It was acknowledged that «incomplete flexicurity leads to the proliferation of unstable contracts and professional insecurity»[19].

Already during that period, Standing wrote that flexicurity had failed in certain states precisely because it had been used as a political justification for the expansion of atypical forms of work, generating what he calls «the new precariat class»[20].

4. The Court of Justice of the EU has established, through numerous judgments, both the manner in which the Directive must be interpreted and the primacy of European Union law over national law.

We consider one of the most important CJEU decisions to be the judgment delivered in Adeneler (C-212/04)[21]. The context of that ruling is the following: Greece had delayed the transposition of Directive 1999/70/EC, and contractual staff within the state budgetary admin-

[18] European Commission, *Employment in Europe Report*, 2006, p. 78 ss.

[19] Eurofound, *Labour market developments*, 2015, p. 44.

[20] G. Standing, *The Precariat. The new dangerous class*, cit., p. 112 ss.

[21] Case C-212/04, *Adeneler and Others v. Ellinikos Organismos Galaktos (ELOG)*, in *https://curia.europa.eu/juris/document/document.jsf;jsessionid=1CF38E87F9D2F9859BCD-466CBB3DADDC?text=&docid=56282&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=13411810*.

istration (the public sector) had been working for years on the basis of fixed-term contracts renewed successively. These contracts were continuously renewed to cover what were permanent needs of the employer, namely the state.

The Adeneler judgment holds, with respect to the application of Clause 5(1)(a) of the Framework Agreement on fixed-term work annexed to Directive 1999/70/EC, that it must be interpreted: «as precluding the use of successive fixed-term employment contracts where the sole justification for such use lies in the existence of a general provision in the primary or secondary legislation of a Member State».

On the contrary, the notion of "objective reasons", within the meaning of this clause, requires that recourse to this particular type of employment relationship, as provided for by national legislation, must be justified by the existence of specific factors, relating in particular to the activity concerned and to the concrete conditions under which it is carried out.

Such a provision, which is purely formal in nature and does not specifically justify the use of successive fixed-term employment contracts by the existence of objective factors linked to the particular characteristics of the activity concerned and to the conditions under which that activity is carried out, entails a real risk of leading to the abusive use of this type of contract and is therefore incompatible with the objective of the Framework Agreement and with the requirement that it produce its useful effect.[22] The conclusion is that the use of successive fixed-term contracts may lead to "a genuine state of precariousness".

In CJEU Case Rosado Santana (C-177/10)[23], the Court held that European legislation (Clause 4 of the Framework Agreement on fixed-term work) must be interpreted as precluding the non-consideration of periods of service completed as an interim civil servant in a public administration when assessing whether such a person – who later be-

[22] Case *Adeneler*, *supra. cit.*, pct. 72.

[23] Case C-177/10, *Rosado Santana v. Consejería de Justicia y Administración Pública de la Junta de Andalucía*, in *https://curia.europa.eu/juris/document/document.jsf?text=&docid=109247&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=13439177*.

came a career civil servant – may obtain an internal promotion reserved exclusively for career civil servants, unless that exclusion is justified by objective reasons within the meaning of Clause 4(1) of that Agreement. The mere fact that the interim civil servant performed those periods of service under a fixed-term employment contract or relationship does not constitute such an objective reason[24].

In this case, «the Spanish Government invokes the existence of several differences between career civil servants and interim civil servants which, in its view, could justify the differentiated treatment at issue in the main proceedings. As regards interim civil servants, the Spanish Government argues, first, that the requirements for access to the civil service and for demonstrating merit and ability are less stringent in their case. Second, it refers to the lack of mobility of interim civil servants, since they are tied to the posts they temporarily occupy, which makes their work different from, and of lower value than, that of a career civil servant. In addition, the Spanish Government submits that certain tasks are reserved for career civil servants, which entails a difference in the quality of their experience and training. Finally, the Spanish Government emphasises that the employment relationship with interim civil servants may be terminated when the need that justified their appointment ceases to exist»[25].

The mere invocation of the temporary nature of the employment relationship of staff of public authorities does not satisfy these requirements and is therefore not, in itself, capable of constituting an "objective reason" within the meaning of Clause 4(1) of the Framework Agreement. If the temporary nature of the employment relationship were considered sufficient to justify a difference in treatment between fixed-term workers and permanent workers, the objectives of Directive 1999/70 and of the Framework Agreement would be deprived of their useful effect, and this would amount to perpetuating a disadvantaged situation for fixed-term workers[26].

[24] Case *Rosado Santana*, *supra. cit.,* point 2 of the operative section of the judgment.

[25] *Idem*, *supra. cit.,* pct. 75.

[26] *Idem*, *supra. cit.,* pct. 74; likewise, the Court has held that Gavieiro Gavieiro and Iglesias Torres, pct. 56 and 57 and the order in Montoya Medina, pct. 42 and 43.

The Court held that Directive 1999/70/EC must be interpreted, on the one hand, as applying to employment contracts and employment relationships concluded with public authorities and other public-sector bodies, and, on the other hand, as precluding any difference in treatment between career civil servants and comparable interim civil servants in a Member State, where such difference in treatment is based solely on the fact that the latter are employed on a fixed-term basis, unless that differential treatment is justified by objective reasons within the meaning of Clause 4(1) of the Framework Agreement.

The Diego Porras case (C-596/14)[27] confirms that fixed-term employment creates an inherent imbalance between the parties. Decided on 14 September 2016, the reasoning in this case contains numerous references to earlier judgments delivered on the basis of Directive 1999/70/EC.

It is worth noting that this judgment further reinforces the interpretation of the concept of "conditions of employment" within the meaning of Clause 4 of the Framework Agreement. The Court held that «a decisive criterion for determining whether a measure falls within the scope of that concept is precisely the criterion of employment, namely the employment relationship established between a worker and his or her employer»[28].

In summary, the Court recalls that the Framework Agreement seeks to apply the principle of non-discrimination and to improve the quality of fixed-term work, and it interprets the notion of "conditions of employment" lato sensu, including within this legal concept elements of remuneration (such as seniority allowances) and conditions governing the termination or expiry of fixed-term employment contracts (notice periods, modalities of termination)[29].

The Court holds that the termination indemnity constitutes a condition of employment, and that Clause 4(1) of the Framework Agreement must therefore be interpreted as meaning that the notion "con-

[27] Case C-596/14, *Diego Porras v. Ministerio de Defensa*, in *https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62014CJ0596*.

[28] Case *Diego Porras*, pct. 22.

[29] *Idem,* pct. 29.

ditions of employment" includes the indemnity owed by the employer to the worker upon the termination of a fixed-term employment contract[30].

Clause 4 of the Framework Agreement precludes a national provision whereby no indemnity is granted to a worker employed under an interinidad (replacement) contract upon its termination, while comparable workers employed under open-ended contracts (and certain other temporary workers) do receive such an indemnity. The mere fact that the work was performed under a fixed-term contract does not constitute an objective reason justifying the refusal to grant the indemnity[31].

We consider that this judgment expands the protection granted to fixed-term workers, strengthening the extensive interpretation of the notion of "conditions of employment", and that EU law thereby limits the margin of discretion of Member States in treating temporary employment regimes differently.

Thus, seemingly simple aspects of the temporality of the employment relationship or the "national legislative tradition" are no longer sufficient grounds to justify less favourable treatment, thereby reinforcing the idea of equalising protection between fixed-term and open-ended contracts whenever the nature of the activity and the working conditions are comparable.

In Case UX v. Governo Italiano and Others (C-658/18)[32], the Court is confronted with a legal situation involving multiple issues that must be resolved.

The category of workers bringing the action before the court consists of Italian justice of the peace judges (giudici di pace). These judges are appointed for a fixed term of four years, renewable, which conceptually places them close to fixed-term workers. The European Court must therefore answer the question: are they "workers" within the meaning of EU law? If the answer is affirmative, they must then be compared with "ordinary judges," who hold open-ended, permanent positions.

[30] *Idem,* pct. 32.

[31] *Idem,* pct. 52

[32] Case C-658/18, *UX v. Governo Italiano and Others*, in *https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62018CJ0658.*

These considerations activate Clauses 4 and 5 of Directive 1999/70, leading to the conclusion that fixed-term workers may not be discriminated against in the absence of an objective reason.

We consider that the time-limited mandate becomes the key element of the entire legal construction: it is not merely a formal aspect, but the objective factor determining the classification of the justice of the peace as a fixed-term worker. It should also be noted that the temporal element is not subject to negotiation and exceeds the usual rules concerning contractual bargaining.

In this context, the CJEU does not discuss the mandate solely in terms of its duration, but as a structural indicator that determines: the nature of the legal relationship, the inclusion or exclusion from the category of "workers," the possibility of comparison with magistrates who have a sui generis permanent employment relationship, and the applicability or non-applicability of the principle of non-discrimination.

In the present case, even though the judicial activity of a justice of the peace is not expressly mentioned in the examples listed in Article 2(1) of Directive 89/391, it nonetheless forms part of the public activity sector. It therefore falls, in principle, within the scope of Directive 89/391 and Directive 2003/88[33].

Under these conditions, it must be considered that Directive 2003/88 is applicable in the main proceedings[34].

That finding is also relevant to the interpretation of the concept of "worker" within the meaning of Article 7 of Directive 2003/88 and Article 31(2) of the Charter, in order to ensure uniformity in the scope ratione personae of workers' right to paid leave (Judgment of 26 March 2015, Fenoll, C 316/13, EU:C:2015:200, paragraph 26)[35].

That concept must be defined according to objective criteria characterizing the employment relationship, taking into account the rights and obligations of the persons concerned.

[33] Case UX, *supra. cit.,* pct. 85.

[34] Case UX, *supra. cit.,* pct. 89.

[35] In the same vein, see the judgment of 20 November 2018, *Sindicatul Familia Constanța and Others*, C 147/17, EU:C:2018:926, paragraph 41.

The question of whether magistrates (judges or prosecutors) are covered by the concept of worker was resolved by the European Court of Justice, and subsequently by the judgment in C-373/24 (Ramavić) of October 30, 2025[36], which ruled that «Article 1 (of Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organization of working time, read in conjunction with Article 31 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that magistrates within the public prosecutor's office fall within the scope of that directive».

This is particularly important because it extends European legal rules to magistrates.

The UX case provides a fair legal solution for a category of workers who have the determining elements of the employment relationship established by law and who, arbitrarily, do not have the same rights as workers in similar situations, but who work under an employment relationship that is not affected by the temporal element.

5. Member States have adopted various mechanisms to prevent abuse: limiting the maximum duration (24–36 months), limiting the number of renewals (1–3), or the condition of "objective reason". Romania is among the most restrictive legally, but enforcement remains deficient. The sanctioning of legal behaviour in the Romanian legal system is the creation of case law, which has established that any breach of a clause expressly provided for by law leads to the conversion of the contract into an indefinite one. Moreover, the lack of a written form leads to such a sanction.

In the Italian legal system, in general, a fixed-term contract can have a duration of up to 12 months without any justification[37].

If the duration exceeds 12 months, the contract may be extended/pseudo-justified, but only up to a maximum of 24 months (including

[36] *https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62024CJ0373&qid=1762514443542.*

[37] *https://iuslaboris.com/insights/italy-recent-changes-to-fixed-term-contracts-and-temporary-agency-work.*

extensions/renewals), provided that a cause is presented, for example: objective temporary necessity, replacement of an absent employee, or temporary and unpredictable increase in the employer's activity[38].

Spain has regulations in place under the Workers' Statute, which stipulates in Article 15 that a contract «is presumed to be concluded for an indefinite period» as a general rule, and that a fixed-term contract «only for production reasons or to replace an employee»[39].

For contracts for production reasons: the maximum duration is 6 months, with the possibility of extension to 12 months if there is a provision in the collective labor agreement concluded at sector level (convenio colectivo) that allows this[40].

If the situation is «short and limited, there may be seasonal or discontinuous» contracts of up to 90 days per calendar year (not continuously)[41].

The French Labor Code regulates fixed-term individual employment contracts in Articles L. 1242-1 et seq.[42]. Such a contract may only be concluded for "temporary" reasons and may not be used to cover a permanent position. Among the accepted reasons are: replacement of an absent employee (maternity leave, illness, vacation, etc.); temporary activity/temporary increase in workload; seasonal work or positions/seasonal jobs: tourism, agriculture, seasonal work, etc.[43].

6. An employment contract is not just a legal document, but a mechanism for distributing social risk. When contractual flexibility is not balanced by protection, the inevitable result is precariousness. Flexicurity is the ideal European solution, but only when security is as strong as flexibility.

The fixed-term individual employment contract is structurally a form of precariousness. Directive 1999/70/EC recognizes the risk, and

[38] *https://www.wfw.com/wp-content/uploads/2018/07/WFW-Briefing-Dignity-Decree-1.pdf.*

[39] *https://www.asesoriacaesar.com/en/real-decreto-32-2021-reforma-laboral-contrato-tiempo-parcial/.*

[40] *https://www.fieldfisher.com/en/insights/key-points-of-the-spanish-labour-reform.*

[41] *https://leglobal.law/2022/03/07/spain-new-provisions-for-temporary-contracts/.*

[42] *https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006901194.*

[43] *https://www.welcometofrance.com/en/fiche/fixed-term-contract.*

the CJEU confirms the vulnerability. Moreover, European statistics highlight the effects.

Excessive use leads to precarious work, which involves one or more dimensions that affect workers. If we were to highlight them, we would not fail to mention the feeling of instability or insecurity regarding job continuity, the lack of individual or collective control over working conditions, remuneration, or working hours. There is a clear lack of sufficient protection against abuse in the workplace and an insufficient level of social protection (access to pensions, health services, etc.). In the long term, there is uncertainty regarding remuneration for work – insufficient and irregular income.

The forms of job security within industrial labor relations, as defined by him, should become elements that also define the legal context of fixed-term individual employment contracts.

Thus, Guy Standing's definitions[44] of labor market security[45], work security/occupational security[46], job security[47], working conditions security[48], skills conversion security[49], income security[50], and representation security[51] must be incorporated into European legislation as general rules that manage, in a unified and community-wide manner, labor relations affected by temporary or atypical elements.

[44] G. Standing, *The Precariat. The new dangerous class*, cit., p. 17.

[45] The existence of adequate income-earning opportunities; at the macro level, this is reflected in the government's commitment to "full employment".

[46] Protection against arbitrary dismissal, regulations on hiring and firing, imposition of costs on employers who do not comply with the rules, and other similar mechanisms.

[47] The ability and opportunity to maintain stable employment, including barriers against skill degradation and opportunities for upward mobility in terms of status and income.

[48] Protection against occupational accidents and illnesses through regulations on occupational safety and health, limits on working time, work at inappropriate hours, night work for women, and compensation in the event of incidents.

[49] The opportunity to acquire skills through apprenticeships, vocational training programs, and other means, as well as the opportunity to effectively use the skills acquired.

[50] Ensuring adequate and stable income, protected by mechanisms such as minimum wages, wage indexation, a comprehensive social security system, progressive taxation to reduce inequalities and supplement low incomes.

[51] Having a collective voice in the labor market through independent trade unions, including the right to strike.

It has been stated that «specific rules applicable to atypical workers, tailored to their vulnerability, appear necessary»[52]. Thus, a more detailed regulation at the European level becomes necessary, one that provides protection for workers in general while also ensuring fair-dealing competition and harmonised regulatory standards within the common market.

7. Technological developments and the increasing digitalisation of the European labour market pose significant challenges to the regulation of fixedterm contracts, highlighting the need to update traditional criteria for classifying atypical employment relationships. The emergence of platformmediated forms of work, the spread of telework and the automation of production processes have made it more common for positions that were traditionally stable to be managed through temporary or flexible contractual arrangements. In this context, the notion of "contract duration" can no longer be understood solely in formal terms, but must be linked to the worker's economic stability, the continuity of earnings, access to opportunities for professional advancement and the protection of social rights.

At the level of the European Union, the recent Directive on platform workers represents a decisive step towards updating the regulatory paradigm: it introduces a legal presumption of employment where elements of control and direction by the platform are present, ensures transparency in the use of automated systems for managing work, and requires the extension of fundamental rights typical of subordinate employment to digital workers. This development entails a systematic reinterpretation of atypical contracts, centred on the actual substance of the employment relationship rather than its formal classification, thereby extending protections previously reserved for stable employment to digitalised and flexible contexts.

From the perspective of social policy, the European Union appears to be moving towards a model of universal protection aimed at reducing structural precariousness even within new forms of employment.

[52] R. Dimitriu, *Labour Law. Anxieties of the Present*, Rentrop & Straton Publishing House, 2016, p. 88.

The integration of continuous training, digital upskilling and reskilling tools is crucial to ensuring that workers can adapt to new production needs, preventing contractual flexibility from resulting in permanent instability. At the same time, greater regulatory harmonisation among Member States can prevent unfair competitive practices based on the systematic use of fixedterm contracts, ensuring the uniform application of the principles of nondiscrimination and worker protection.

Ultimately, recent regulatory and technological developments outline a new horizon for fixedterm contracts in the European Union: no longer confined to traditional temporary employment relationships, but extending to digitalised and platformmediated forms of work, with the aim of ensuring social security, fairness and continuity of fundamental rights, even within the emerging cyberspace of the European labour market.

Le Autrici e gli Autori

Giorgi Amiranashvili, *Assistant Professor, Head Specialist (I Category), Department of Internationalization and Scientific Research, Faculty of Law, Tbilisi State University*

Valentina Barela, *Associata di Diritto privato comparato, Dipartimento di Scienze giuridiche, Università di Salerno*

Giorgia Bevilacqua, *Ricercatrice di Diritto internazionale, Dipartimento di Giurisprudenza, Università Vanvitelli*

Pasquale Borrata, *Contrattista progetto Sec-CO-OC*

Veronica Caporrino, *Associata di Diritto privato comparato, Dipartimento di Giurisprudenza, Università Vanvitelli*

Gisella Emma Comes, *Dottoressa di ricerca, Dipartimento di Giurisprudenza, Università Vanvitelli e Contrattista progetto Sec-CO-OC*

Federica De Simone, *Docente incaricato di Criminologia, Dipartimento di Giurisprudenza, Università Vanvitelli e Assegnista di ricerca progetto Sec-CO-OC*

Carmen Di Carluccio, *Associata di Diritto del lavoro, Dipartimento di Giurisprudenza, Università Vanvitelli*

Katia Fiorenza, *Associata di Diritto privato comparato, Dipartimento di Diritto, Economia, Management e Metodi Quantitativi, Università del Sannio*

Ilaria Infante, *Dottoressa di ricerca, Dipartimento di Giurisprudenza, Università Vanvitelli e Contrattista progetto Sec-CO-OC*

Eva Lacková, *Postdoctoral Researcher, Faculty of Law, Pavol Jozef Šafárik University e Contrattista progetto Sec-CO-OC*

Alessandro Leopizzi, *Avvocato e Dottore di ricerca in Diritto internazionale, Dipartimento di Scienze umane e sociali, Università del Salento*

Constanța Mătușescu, *Associate Professor, PhD, Faculty of Law and Administrative Sciences, Valahia University of Targoviste*

Marius Mihălăchioiu, *Lecturer PhD, Faculty of Law and Administrative Sciences, Valahia University of Targoviste, Judicial assistant, The Court of Dâmbovița County*

Juan Carlos García Quiñones, *Full Professor of Labour Law and Social Security Law, Faculty of Law, Complutense University of Madrid*

Massimiliano Rak, *Ordinario di Sistemi di elaborazione delle informazioni, Dipartimento di Ingegneria elettrica e tecnologie dell'informazione, Università Federico II*

Denisa Rudžiková, *Assistant Professor, Department of Labour Law and Social Security Law, Faculty of Law, Pavol Jozef Šafárik University*

Livia Saporito, *Ordinaria di Diritto privato comparato, Dipartimento di Giurisprudenza, Università Vanvitelli*

Antonello Tipaldi, *Docente a contratto e didattica integrativa di Diritto commerciale*, *Dipartimento di Scienze Aziendali Management & Innovation Systems, Università di Salerno*

Dan Țop, *già Full Professor Faculty of Law and Administrative Sciences, Valahia University of Targoviste, President Association for the Study of the Professional Labour Relations*

Antonio Vertuccio, *Dottore di ricerca, Dipartimento di Giurisprudenza, Università Vanvitelli e Contrattista progetto Sec-CO-OC*

Tamar Zarandia, *Associate Professor of Civil law and Dean, Faculty of Law, Tbilisi State University*

Volumi pubblicati nella Collana

1. Di Carluccio C., Festa A. (a cura di), *Il lavoro tra transizione ecologica e digitale. Esperienze europee a confronto*, 2024.
2. De Simone F., *Nuove coordinate in tema di prevenzione e contrasto della corruzione*, 2025.
3. Di Carluccio C., Festa A. (a cura di), *Digitalizzazione del lavoro inclusività e Work-Life- Balance. Un itinerario di ricerca multidisciplinare*, 2025.
4. Sorvillo F. (a cura di), *Gaming ed e-sports tra diritto, religioni e culture. Profili multidisciplinari ed esperienza giuridica*, 2025.

Finito di stampare nel mese di dicembre 2025
Presso la *Grafica Elettronica* – Napoli