ISSN: 2704-8012

SUOR ORSOLA
BENINCASA
UNIVERSITÀ EDITRICE

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu



2025/2

EJPLT
ISSN: 2704-8012

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2025/2

SUOR ORSOLA BENINCASA
UNIVERSITÀ EDITRICE

European Journal of Privacy Law & Technologies
Italian R.O.C. n. 25223
ISSN: 2704-8012

On line journal
https://doi.org/10.57230/EJPLT https://doi.org/10.57230/EJPLT252

Web (free access)
www.ejplt.tatodpr.eu

Contacts
ejplt@unisob.na.it +39 081.2522396

Indexed in

























EJPLT has been awarded Class A status by ANVUR. The journal is Open Access Diamond and is the scientific dissemination tool of the Research Centre in European Private Law (ReCEPL).

The Journal was born in 2018 as one of the results of the European project "Training Activities to Implement the Data Protection Reform" (TAtoDPR – 2017-2019), co-funded by the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

From 2019-2022, the Journal was supported by the Erasmus+ Programme of the European Commission within the European Project Jean Monnet Chair 'European Protection Law of Individuals in relation to New Technologies' (PROTECH) (Call: EAC/A03/2018 – Project n. 611876-EPP-1-2019-1-IT-EPPJMO-CHAIR).

From 2022-2025 EJPLT has been further implemented thanks to the Jean Monnet Chair project 'European Green Rights: reshaping fundamental rights for next generations' (EUGREENEXT) (ERASMUS-JMO-2021-HEI-TCH-RSCH – Proposal n. 101047962).

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The Issues form 2018/1 to 2020/1 were published by Giappichelli Publisher.
From Issue 2020/2 the Publisher is Suor Orsola Benincasa Università editrice.

Code of Ethics: universitypress.unisob.na.it/ojs/index.php/ejplt/pages/view/codiceetico

Editing
Luciana Trama

Design
Flavia Soprani

Development
Maria Teresa Lo Conte

© Copyright 2025 by Suor Orsola Benincasa Università Editrice, published in December 2025
The intellectual property of the individual contributions remain with the authors.
The Issue and the individual contributions are licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND. All the details at: https://creativecommons.org/licenses/by-nc-nd/4.0.

European Journal of Privacy Law & Technologies Committee

EDITOR IN CHIEF/DIRECTOR

Prof. Avv. Lucilla Gatt, Università degli Studi Suor Orsola Benincasa di Napoli, Italy

VICE-DIRECTOR

Prof. Ilaria A. Caggiano, Università degli Studi Suor Orsola Benincasa di Napoli, Italy

COORDINATOR OF THE EDITORIAL AND REFEREES BOARD

Ph.D. Avv. Maria Cristina Gaeta, Università degli Studi Suor Orsola Benincasa, Italy

ADVISORY BOARD – SCIENTIFIC COMMITTEE

Prof. Pasquale Arpaia, Università degli Studi di Napoli Federico II, Italy
Prof. Giovanna Capilli, Università San Raffaele di Roma, Italy
Prof. Aurelia Colombi Ciacchi, University of Groningen, Netherlands
Prof. Jean-Sébastien Borghetti, Université Panthéon-Assas, France
Prof. Matthew Dyson, University of Oxford, United Kingdom
Prof. Valeria Falce, Università Europea di Roma, Italy
Prof. Indranath Gupta, O.P. Jindal Global University, India
Porf. Juan Ernesto Gutiérrez Otiniano, Universidad Autonoma del Perù, Peru
Prof. Pim Haselager, Radboud University, Netherlands
Prof. Toni Jaeger-Fine, Fordham University School of Law, United States
Prof. Antonios Karaiskos, Ryukoku University, Japan
Prof. Jingkun Liu, China University of Political Science and Law, China
Prof. Roberto Montanari, Università degli Studi Suor Orsola Benincasa, Italy
Prof. Roberta Montinaro, Università degli Studi di Napoli l'Orientale, Italy
Prof. Juan Pablo Murga Fernandez, Universidad de Sevilla, Spain
Prof. Nora Ni Loideain, Institute of Advanced Legal Studies of London, United Kingdom
Prof. Alex Nunn, Leeds Trinity University, United Kingdom
Prof. Avv. Salvatore Orlando, Sapienza Università di Roma, Italy
Prof. Vincenzo Ricciuto, Università degli Studi di Roma Tor Vergata, Italy
Prof. Emilio Tosi, Università degli Studi di Milano Bicocca, Italy

REFEREES

Prof. Carlos Antonio Agurto Gonzáles, Universidad Nacional Mayor de San Marcos, Peru
Prof. Jaime Alcalde Silva, Pontificia Universidad Católica de Chile, Chile
Prof. Miguel Álvarez Ortega, Kyoto University, Japan, and Universidad de Sevilla, Spain
Prof. Julio Álvarez Rubio , Universidad de Cantabria Santander, Spain
Prof. Jeremy Antippas, Université de Bretagne Sud, France
Prof. Mahmood Bagheri, Institute of Advanced Legal Studies of London, United Kingdom
Prof. Marco Bassini, Tilburg University, Netherlands
Prof. Ettore Battelli, Università Roma Tre, Italy
Prof. Claudia Benanti, Università di Catania, Italy
Prof. Andrea Bertolini, Scuola Superiore Sant'Anna di Pisa, Italy
Prof. Consiglia Botta, Università degli Studi di Napoli Federico II, Italy
Prof. Cristina Caricato, Sapienza Università di Roma, Italy
Prof. Roberto Carleo, Università degli Studi di Napoli Parthenope, Italy
Prof. Georges Cavalier, Université de Lyon, France
Prof. María Dolores Cervilla Garzón, Universidad de Càrdiz, Spain
Prof. Alberto Giulio Cianci, Università degli Studi di Perugia, Italy

European Journal of Privacy Law & Technologies Committee

Prof. Maria Antonia Ciocia, Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Giuseppe Corasaniti, Universitas Mercatorum e Luiss, Italy
Prof. Lucila Inés Córdoba, Universidad de Buenos Aires, Argentina
Prof. Valentina Vincenza Cuocci, Università di Foggia, Italy
Prof. Giovanna D'Alfonso, Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Egidio De Benedetto, Università degli Studi di Napoli Federico II, Italy
Prof. Carlos de Cores Helguera, Universidad CLAEH del Uruguay, Uruguay
Prof. Valentina Di Gregorio, Università di Genova, Italy
Prof. Giuseppe Di Vetta, Scuola Universitaria Superiore Sant'Anna di Pisa, Italy
Prof. Alessandro Ferrero, Politecnico di Milano, Italy
Prof. Manuel Espejo Lerdo de Tejada, Universidad de Sevilla, Spain
Prof. Elżbieta Feret, Uniwersytet Rzeszowski, Poland
Prof. Gianluca Gentile, Università degli Studi di Napoli Suor Orsola Benincasa, Italy
Prof. Marco Giacalone, Vrije Universiteit Brussel, Belgium
Prof. Gina Gioia, Università degli Studi della Tuscia, Italy
Prof. Maren Heidemann, London Centre for Commercial and Financial Law, United Kingdom
Prof. Giovanni Iorio, Università degli Studi di Milano Bicocca, Italy
Prof. Jorge Antonio Jimenez Carrero, Universidad Europea Madrid, Spain
Prof. Arndt Künnecke, Hochschule des Bundes für öffentliche Verwaltung, Germany
Prof. Antonio Las Casas, Università di Catania, Italy
Prof. Jingkun Liu, China University of Political Science and Law, China
Prof. Leysser Luggi Leon Hilario, Pontificia Universidad Católica del Perú, Peru
Prof. Paola Manes, Alma Mater Studiorum Università di Bologna, Italy
Prof. Giovanni Martini, Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Stefano Mauro, Politecnico di Torino, Italy
Prof. Michala Meiselles, University of Derby, United Kingdom
Prof. Alessia Mignozzi, Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Salvatore Monticelli, Università di Foggia, Italy
Prof. Cinzia Motti, Università di Foggia, Italy
Prof. Beth Nosworthy, University of Adelaide, Australia
Prof. Taiwo Oriola, University of Derby, United Kingdom
Prof. Francesco Rossi, Università degli Studi di Napoli Federico II, Italy
Prof. Gemma Rubio, Universitat de Barcelona, Spain
Prof. Silvia Salardi, Università degli Studi di Milano Bicocca, Italy
Prof. Fulvio Santarelli, Universidad de Palermo, Argentina
Prof. Romina Santillan Santa Cruz, Universidad de Zaragoza, Spain
Prof. Serena Sileoni, Università degli Studi Suor Orsola Benincasa, Italy
Prof. Carla Solinas, Università degli Studi di Roma Tor Vergata, Italy
Prof. Natalia Shyriaieva, National Technical University Kharkiv Polytechnic Institute, Ukraine
Prof. Avv. Laura Valle, Libera Università di Bolzano, Italy
Prof. Jiao Xue, Zhejiang Police College, China
Prof. Lihong Zhang, East University of Political Science and Law, Shanghai, China
Prof. Isabel Zurita Martin, Universidad de Cádiz, Spain

EDITORIAL BOARD

Ph.D. (c) Maria Teresa Lo Conte, Journal Design&Innovation Officer – Università degli Studi di Roma Tor Vergata, Italy
Prof. Sara Lorenzo Cabrera, Universidad de La Laguna, Spain

European Journal of Privacy Law & Technologies

Committee

Prof. Manuel Pereiro Càrceles, University of Valencia Universidad Complutense de Madrid, Spain
Prof. Carlo Ciliberto, University College London, United Kingdom
Prof. Maria Ioannidou, Queen Mary University of London, United Kingdom
Prof. André Janssen, Radboud University Nijmegen, Netherlands
Prof. David T. Karamanukyan, Siberian University, Russian Federation
Prof. Jacopo Martire, University of Bristol, United Kingdom
Prof. Avv. Alessandra Sardu, Università degli Studi di Modena e Reggio Emilia, Italy
Prof. Hakeem Yusuf, University of Derby, United Kingdom
Ph.D. Avv. Mark Giancaspro, University of Adelaide, Australia
Ph.D. Avv. Livia Aulino, Università degli Studi di Napoli Federico II, Italy
Ph.D. Irene Coppola, Università degli Studi Suor Orsola Benincasa di Napoli, Italy
Ph.D. Avv. Lorenzo Corea, Università di Pisa, Italy
Ph.D. Avv. Andrea D'Alessio, Università degli Studi di Teramo, Italy
Ph.D. Davide D'Aloia, Università degli Studi Suor Orsola Benincasa, Italy
Ph.D. Domenico Fauceglia, Università degli Studi di Roma Tor Vergata, Italy
Ph.D. Avv. Caterina del Federico, Alma Mater Studiorum Università di Bologna, Italy
Ph.D. Matteo Fermeglia, Hasselt University, Belgium
Ph.D. Paola Giacalone, Università degli Studi Suor Orsola Benincasa and Vrije Universiteit Brussel, Belgium
Ph.D. Avv. Paola Grimaldi, Università degli Studi della Campania Luigi Vanvitelli, Italy
Ph.D. Dorota Habrat, Uniwersytet Rzeszowski, Poland
Ph.D. Avv. Aldo Iannotti della Valle, Università degli Studi Suor Orsola Benincasa, Italy
Ph.D. Avv. Valeria Manzo, Università degli Studi della Campania Luigi Vanvitelli, Italy
Ph.D. Avv. Anita Mollo, Scuola Superiore Meridionale, Italy
Ph.D. Avv. Michael William Monterossi, Università di Torino, Switzerland
Ph.D. Ph.D. Hans Steege, University of Stuttgart, Germany
Ph.D. Kamil Szpyt, Andrzej Frycz Modrzewski Krakow University, Poland
Ph.D. Emiliano Troisi, Università Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Noel Armas Castilla, Universidad de Sevilla, Spain
Ph.D.(c) Avv. Giuseppe Bova Crispino, Università Luiss Guido Carli, Italy
Ph.D. (c) Florencia Ines Cordoba, Universidad de Buenos Aires, Argentina
Ph.D. (c) Alessandra Fabrocini, Sapienza Università di Roma, Italy
Ph.D. (c) Andrea Filippo Ferraris, Alma Mater Studiorum Università di Bologna and Vrije Universiteit Brussel, Belgium
Ph.D. (c) Gabriela García Vera, Uniwersytet Rzeszowski, Poland
Ph.D. (c) Simona Ghionzoli, Università degli Studi di Napoli l'Orientale, Italy
Ph.D. (c) Ludovica Maria Giordano, Sapienza Università di Roma, Italy
Ph.D. (c) Pablo Guédon, Université Clermont Auvergne, France
Ph.D. (c) Luigi Izzo, Università degli Studi Suor Orsola Benincasa, Italy
Ph.D. (c) Marianna Molinari, Alma Mater Studiorum Università di Bologna and Vrije Universiteit Brussel, Belgium
Ph.D. (c) Marie Potus, Université Marie et Louis Pasteur, France
Ph.D. (c) Giovanni Russo, L.U.I.S.S. Guido Carli, Italy
Ph.D. (c) Michele Scotto di Carlo, Università degli Studi di Napoli Federico II, Italy
Ph.D. (c) Chiara Vitagliano, Università degli Studi di Napoli l'Orientale, Italy
Ph.D.(c) Ruichen Zhang, Sapienza Università di Roma and Zhongnan University of Economics and Law, China

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES
2025/2

Summary

Articles

Developing Civil Liability for Cyber Breaches in Palestine: An Analytical Study in Light of Comparative Law | Sviluppo della responsabilità civile per le violazioni informatiche in Palestina: uno studio analitico alla luce del diritto comparato
Anas Abu Aloun

Measuring contract transparency: from legal reasoning to LLM-based assessment. An italian law perspective | Misurare la trasparenza contrattuale: dal ragionamento giuridico all'impiego dei modelli linguistici. Una prospettiva di diritto italiano
Ilaria Amelia Caggiano

The expanding notion of special categories of data and its limits | L'espansione della nozione di categorie speciali di dati e i loro limiti
Anna Capellà i Ricart, Antoni Roig Batalla

Some remarks on nanotechnologies, safety and product liability | Alcune osservazioni su nanotecnologie, sicurezza e responsabilità da prodotto
Giovanna Capilli

Il Greenwashing: asimmetrie di mercato e interventi normativi nell'Unione Europea | Greenwashing: market asymmetries and regulatory measures in the European Union
Maria Antonia Ciocia

Artificial Intelligence in the EU Digital Market: Data Circulation and Fundamental Rights Protection | Intelligenza artificiale nel mercato digitale dell'UE: circolazione dei dati e tutela dei diritti fondamentali
Valentina Di Gregorio

Responsabilidad algorítmica y el sujeto artificial: hacia un modelo funcional de imputación jurídica en entornos digitales de consumo | Algorithmic liability and the artificial subject: Towards a functional model of legal attribution in digital consumer environments
Marcos Daniel Di Loreto

Instances of legal subjectivity between the natural and artificial worlds: the new content of the legal subjectivity of the natural human being in a perspective of protection of vulnerability as the authentic content of sustainability | Istanze di soggettività giuridica tra mondo naturale e artificiale: il nuovo contenuto della soggettività giuridica dell'essere umano naturale in una prospettiva di tutela della vulnerabilità come autentico fondamento della sostenibilità
Lucilla Gatt

Analysis and perspectives on the AI Act: scope and impact assessment | Analisi e prospettive dell'AI Act: ambito di applicazione e valutazione d'impatto
Lucilla Gatt, Maria Teresa Lo Conte, Maria Eugenia Mazzarella

La nuova Legge Quadro per lo Spazio: una innovazione per l'Italia | The new Framework Law for Space: an innovation for Italy
Lucilla Gatt, Andrea Taramelli, Luigi Izzo, Carlo Candeloro Campanile

The Fog of Information: the EU AI Act and legal strategies against AI-fuelled disinformation | La nebbia dell'informazione: l'AI Act dell'UE e le strategie giuridiche contro la disinformazione alimentata dall'IA
Eleni Gavriil, Georgios Pavlidis

Obbligo di riparazione del bene acquistato dal consumatore e sostenibilità | Obligation to repair purchased goods by consumers and sustainability
Arturo Maniaci

The contract as a tool for conflict management: procedural agreements and digital Innovation | Il contratto come strumento di gestione del conflitto: accordi procedurali e innovazione digitale
Lurdes Varregoso Mesquita

GDPR and Blockchain technologies: a complex relationship | GDPR e tecnologie blockchain: una relazione complessa
Enza Pellecchia

The role of the certification systems in the EU legal framework for sustainability goals, current state and future perspectives | Il ruolo dei sistemi di certificazione nel quadro giuridico dell'UE per gli obiettivi di sostenibilità, situazione attuale e prospettive future
Laura Valle

Focus

Smart Contracts for Online Dispute Resolution: Legal Implications and Practical Applications under EU regulations | Gli Smart Contract per la risoluzione online delle controversie: implicazioni giuridiche e applicazioni pratiche alla luce del quadro normativo dell'Unione Europea
Gioia Arnone

The Kleinberg epistemic paradox within contractual discrimination | Il paradosso epistemico di Kleinberg e la discriminazione contrattuale
Giovanni Battaglino

Il token immobiliare nel contesto del codice civile italiano | The real estate token in the context of the Italian civil code
Davide Silvio D'Aloia

Provocazioni culturali e implicazioni giuridiche degli AI Companion | Cultural Provocations and legal implications of AI Companions
Antonella Di Cerbo

AI-driven Healthcare and Contracts | Assistenza sanitaria e contratti fondati sull'IA
Stefania Pia Perrino

Redefining "Reasonable Harm" to Privacy in the Digital Surveillance Era: A Critical Analysis of Israeli Legal Framework | Ridefinire il 'danno ragionevole' alla privacy nell'era della sorveglianza digitale: un'analisi critica del quadro giuridico israeliano
Eyal Sabro, Bartolomé Torralbo Muñoz

Analisi della comunicazione pubblicitaria: mercato e diritti fondamentali | Analysis of advertising communication: market and fundamental rights
Andrea Senatore

List of authors

SECTION I
ARTICLES

Abu Aloun A, 'Developing civil liability for cyber breaches in Palestine: an analytical study in light of comparative law' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252AAA

EJPLT
ISSN 2704-8012



Developing civil liability for cyber breaches in Palestine: an analytical study in light of comparative law

Sviluppo della responsabilità civile per le violazioni informatiche in Palestina: uno studio analitico alla luce del diritto comparato

ANAS MOUSA ABU ALOUN
Associate Professor of Civil Law
Arab American University

Abstract

The paper analyses the influence of the Palestinian legal system on the breach of data and cyberattacks. The main problem is the dependence of Palestinian legislation on a statute that was passed during the British Mandate in 1944, which is known as British Civil Wrongs Ordinance. The age of this law makes it inadequate for current technological advancements. The research problem mainly revolved around how to adapt the rules of this obsolete ordinance to modern times. The researcher came to the conclusion that a person who wishes to claim compensation as a result of a cyberattack must establish three parts of liability, namely: a legal duty to protect the concerned personal data existed, that the data protector was negligent which resulted in the harm, and that there was actual harm due to the breach. To come up with a suitable law for Palestine, the researcher made a comparison between the Palestinian and the modern laws like the European General Data Protection Regulation (GDPR) and the UK Data (Use and Access) Act 2025. The researcher noted many differences between these laws and the Palestinian law, which include among others the lack of a clear right to compensation for non-material damage in the Palestinian law as well as the difficulty in assigning liability when several parties are involved and the absence of legal regulation on reasonable security measures that should be in place to prevent such breaches. The study made the argument for the amendment of laws by proposing changes that are in line with the recognized international standards, and offering training to those in the legal field to increase their knowledge of cybersecurity issues and their implications.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Lo studio affronta la questione di come la legislazione palestinese affronti le violazioni dei dati e gli attacchi informatici. La difficoltà risiede nella dipendenza della legislazione palestinese da una legge emanata durante il Mandato britannico nel 1944 (il British Civil Wrongs Ordinance). L'antichità di questa legge la rende incapace di affrontare gli attuali sviluppi tecnologici. Il principale problema di ricerca era come adattare le regole del British Civil Wrongs Ordinance del 1944, che rimane in vigore in Palestina.
Il ricercatore ha concluso che qualsiasi individuo che intenda presentare una richiesta di risarcimento derivante da attacchi informatici deve dimostrare tre elementi di responsabilità: l'esistenza di un obbligo legale di proteggere i dati personali, la negligenza da parte della persona responsabile della protezione dei dati che ha portato al verificarsi del danno, e il verificarsi del danno come risultato della violazione.
Al fine di sviluppare la legislazione palestinese, il ricercatore ha confrontato la legge palestinese con sistemi avanzati come il Regolamento Generale sulla Protezione dei Dati europeo (GDPR) e il Data (Use and Access) Act 2025 del Regno Unito. Il ricercatore ha riscontrato differenze significative tra queste leggi e la legge palestinese, tra cui l'assenza nella legge palestinese di un diritto chiaro al risarcimento per danni non materiali, la difficoltà nell'attribuire la responsabilità quando sono coinvolti più soggetti, e la mancanza di regolamentazione nella legge palestinese riguardo alle misure di sicurezza ragionevoli che dovrebbero essere adottate per prevenire tali violazioni.
Lo studio ha proposto emendamenti legislativi derivati da standard internazionali riconosciuti, nonché la formazione per coloro che operano nel settore legale al fine di ampliare le conoscenze sulle questioni di cybersecurity e sulle loro implicazioni.

Keywords: Cyber Liability; Civil Wrongs Ordinance; Palestine; Data Protection; Duty of Care; Causality; Comparative Law

Summary: 1. Introduction. – 2. Due Diligence in Cybersecurity under British Law. – 2.1. The Role of the UK GDPR and the Data Protection Act 2018 in the UK in Developing the Concept of Due Diligence. – 2.2. The Civil Wrongs Ordinance and the Draft Data Protection Law of 2025. – 2.3. Special Conditions for Considering an Act a Civil Wrong in the Context of Personal Data Protection. – 3. The Element of Damage in Cyber Liability Cases (From Tangible to Intangible Damages). – 3.1. Material (Tangible) Damage in Cyber Liability Cases. – 3.2. Moral Damage in Cyber Breaches. – 4. Legal Integration Between Articles 60 and 55 bis in Addressing Causality. – 4.1. Article 60 of the Palestinian Civil Wrongs Ordinance Provides a Solid Legal Framework for Linking Compensation to Causality. – 4.2. Enhancing Integration Between Article 60 and Articles 50 and 55 bis. – 5. Conclusion.

1. Introduction.

The rapid digitisation of Palestinian society – from mobile banking and e-government services to online education and health records – has brought

undeniable convenience.[1] Yet it has also made individuals and institutions vulnerable to cyber threats that are unprecedented in their scope and sophistication.[2] When personal information is stolen, money is drained from bank accounts, and intimate photos are shared, it is not a hypothetical problem; it is a living reality for ordinary citizens. The tragedy is that the legal tool most readily available to seek redress – the British Civil Wrongs Ordinance of 1944, as amended in 1947 – was drafted in an era when "data" meant paper files locked in cabinets. The question this study asks is therefore both simple and urgent: can a statute born in the Mandate period still deliver justice in the age of ransomware and state-sponsored hacking?

The answer, as the following pages demonstrate, is that it can – but only with considerable creativity, comparative borrowing, and, ultimately, legislative courage.

This research proceeds by placing the Ordinance in direct conversation with three far more modern frameworks: – the United Kingdom's post-Brexit regime (UK GDPR and Data Protection Act 2018, now being substantially reshaped by the Data (Use and Access) Act 2025 that entered into force on 19 June 2025); – the risk-based U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework; and – the ambitious yet still unfinished Palestinian Draft Data Protection Law of 2025.

The comparison is rather revealing. The law of Palestine uncovers three main weaknesses, namely: first, there is no reliable way for victims to get compensated for non-material damage (psychological distress and loss of privacy which have become the two major claims today); secondly, the situation is unclear when it comes to sharing responsibility of the case when there are many parties involved and all of them have contributed to the violation; thirdly, there are virtually no objective criteria for "reasonable security measures" at all. The absence of these benchmarks marginalizes the victims - either they are individuals or small enterprises - with remedies that seem to exist in theory but are practically impossible to obtain.

Yet the Ordinance is not a dead letter. Articles 50 (negligence), 55 bis (breach of statutory duty), and 60 (assessment of damage) retain remarkable elasticity. When read creatively – and in light of international precedents such as the £20 million British Airways penalty (2020) and the $575 million Equifax settlement (2019) – they can be pressed into service today. The Draft Data Protection Law 2025, once enacted, will supply the missing statutory duties; Article 55 bis can then transform their violation into an actionable civil wrong, bridging an eighty-year gap with surprising elegance.

Therefore, the main question that the research attempts to answer is: Can the rules of the British Civil Wrongs Ordinance frame liability for cyberattacks? What are the obstacles that prevent its application?

These questions will be answered using the analytical and comparative methods, thereby enabling the proposal of amendments to the British Civil

[1] Palestinian Central Bureau of Statistics, 'ICT Survey on Households and Individuals 2024' (Ramallah, PCBS 2025) (showing 87 % smartphone penetration and 72 % use of e-banking services). <https://www.pcbs.gov.ps/PCBS-Metadata-en-v5.2/index.php/catalog/733>

[2] See, eg, Human Rights Watch, '*A Threshold Crossed: Israeli Authorities and the Crimes of Apartheid and Persecution*' (HRW 2021) ch VII (on weaponised data leaks and doxing campaigns).

Wrongs Ordinance in force in Palestine to address cyber liability, and examining the extent to which the Palestinian Data Protection Draft Law provides comprehensive protection against cyberattacks.

2. Due Diligence in Cybersecurity under British Law.

The principle of the "duty of care" is considered the fundamental element in establishing civil liability arising from negligence, particularly in Anglo-Saxon legal systems, of which the British Civil Wrongs Ordinance in force in Palestine forms an integral part, as all its provisions are derived from this system. In light of the complex cyber-attacks, can this principle, as stipulated in the British Civil Wrongs Ordinance in force in Palestine, confront the complexities resulting from these attacks?

This part of the research aims to study this principle according to its modern concept, which has evolved in its original system in the United Kingdom, which has adopted a data protection system for 2018 and the Data (Use and Access) Act 2025. This is what we will address in:

- Section One: The Role of the UK GDPR and the Data Protection Act 2018 in the UK in Developing the Concept of Due Diligence; and
- Section Two: The Civil Wrongs Ordinance and the Draft Data Protection Law of 2025.

2.1. The Role of the UK GDPR and the Data Protection Act 2018 in the UK in Developing the Concept of Due Diligence.

The duty of care is the cornerstone of the tort of negligence. It obliges every person (whether natural or legal) to take reasonable measures to prevent foreseeable harm that may befall others who can reasonably be expected to be affected by their acts or omissions. The contemporary law of negligence has its roots in the leading case of Donoghue v Stevenson.[3] The “Neighbour Principle” formulated by Lord Atkin continues to be the ideological foundation of the duty of care principle., which remains to this day the philosophical and legal bedrock for determining when a duty of care arises. The classic formulation (almost poetic) formulation from Lord Atkin’s judgment: “You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who, then, in law is my neighbour? The answer is: persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question.” From the above, the duty of care is composed of three essential elements:

Reasonable care What the “reasonable and prudent person” would have done in the same circumstances – neither perfection nor indifference is required.

The neighbour = the reasonably foreseeable victim Any person (physically, functionally, or relationally proximate) whom it is reasonably foreseeable

[3] Donoghue v Stevenson [1932] AC 562 (HL).

would be directly harmed by your act or omission – even if you do not know their name.

Ought to be in your contemplation reasonably You do not have to have personal acquaintance with the particular person; it is enough that a hypotheti-cal person in your place could predict that a person similar to the plaintiff's might be harmed.

In the context of cybersecurity, this principle translates into an obligation for organizations to protect personal data and digital systems from various threats, including:

- Malware: Programs designed to steal data or damage systems, as in the Emotet attack (2020), which targeted banks and government institutions.[4]
- Phishing: Attempts to deceive users via fake emails or websites to obtain sensitive data, such as login credentials.
- Ransomware: Encrypting data and demanding a ransom for its release, as in the NotPetya attack (2017), which caused enormous global losses.[5]
- DDoS attacks: in essence, inundating a system with bogus requests to the point of collapse, similar to the 2016 Dyn attack that caused Twitter and Netflix to be unavailable for hours. The duty of care principle application in the cybersecurity context is reliant on a meticulous risk evaluation that takes into account data sensitivity, threat level, and security measures cost as the main factors.

Sensitive data, such as electronic health data subject to HIPAA or financial data, requires stricter security measures compared to public data like email addresses.[6] The threat level also varies according to the nature of the attacks; targeted attacks (Advanced Persistent Threats) require the use of advanced systems like Intrusion Detection Systems (IDS), while firewalls are sufficient to counter random attacks. [7] At the same time, security measures must be economically feasible, considering the principle of proportionality, as applying Security Information and Event Management (SIEM) systems may be costly for small companies but necessary for large institutions managing sensitive data.[8]

In this context, reasonable security measures that entities responsible for data protection must take to fulfil their duty of care obligations include: Encryption using standards like AES-256 to protect data in transit and at rest, reducing the risk of leakage [9] Multi-Factor Authentication (MFA), which combines passwords, temporary codes, or biometric identifiers to prevent

[4] 'Attack Chain Overview: Emotet in December 2020 and January 2021' (Unit42, Palo Alto Networks, 20 January 2021) <https://unit42.paloaltonetworks.com/attack-chain-overview-emotet-in-december-2020-and-january-2021/> accessed 4 September 2025.

[5] 'NotPetya (2017)' (CCDCOE) <https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)> accessed 4 September 2025.

[6] J Kosseff, *Cybersecurity Law* (3rd edn, Wiley 2024) 145–147.

[7] R Ross, *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication 800-53 Rev 5, NIST 2020).

[8] B Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (WW Norton & Company 2018).

[9] A Solow-Niederman, 'Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches' (2018) 127 Yale Law Journal Forum 614.

unauthorised access[10] Security Information and Event Management (SIEM) systems that monitor systems in real-time to detect threats and log incidents to accelerate response; and finally, regular software updates by applying security patches to address vulnerabilities, as was the case with the Log4j vulnerability in 2021 that affected millions of systems.[11] .When you actually implement all of these things properly, they do actually strengthen your defenses against breaches of cyber security, while at the same time helping to ensure that you're discharging your duty of care that goes back to the classic case of Donoghue v Stevenson.[12]

The UK GDPR and similar legal and technical regulatory frameworks have a significant impact on cybersecurity. They impose clear and firm data protection standards rather than mere uncertain promises. These measures have practically compelled the parties involved in data handling to be serious and professional about security, such as using proper encryption, installing strict access controls, and even formulating incident-response plans, among others[13].

That way they cut down the chances of a breach and, more importantly, they can show they're not falling short on the duty of care they owe everyone.[14] If you link liability to actual technical defences like that, the whole thing forces everybody to stop reacting after the mess has happened and start protecting sensitive data properly before the hackers turn up. That's exactly the spirit of negligence law that was started by Donoghue v Stevenson nearly a century ago, and it works beautifully with how we try to run cybersecurity these days.

UK GDPR and Data Protection Act 2018 essentially give us a pretty solid legal backbone that ensures everyone handling personal data steps up their game in terms of their duty of care and throws down some pretty tough regulations in terms of cybersecurity and compliance. Article 32 of the UK GDPR states that:

" 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a)the pseudonymisation and encryption of personal data;

(b)the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c)the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d)a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from

[10] DJ Solove, PM Schwartz, *Data Protection Law* (2nd edn, Wolters Kluwer 2020).
[11] A Wirth, 'Log Jam: Lessons Learned from the Log4Shell Vulnerability' (2022) 56 Biomedical Instrumentation & Technology 72.
[12] Donoghue (n 1).
[13] N Kshetri, 'The Log4j Vulnerability: Impacts and Lessons for Cybersecurity Governance' (2022) 2 Journal of Cybersecurity and Privacy 123; UK General Data Protection Regulation, art 32.
[14] ibid; P Carey, *Data Protection: A Practical Guide to UK and EU Law* (6th edn, OUP 2022).

accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by".

Furthermore, Article 33 of the UK GDPR sets a rather tight deadline: once a controller becomes aware of a personal data breach that is likely to pose a risk to individuals' rights and freedoms, it must notify the supervisory authority (in the UK, the ICO) within 72 hours. There is very little room for delay.

Article 82 takes this a step further by actually granting data subjects a right to compensation. This includes not only material damage (such as actual monetary losses due to fraud or identity theft) but also non-material damage (such as the distress and anxiety that often accompany a major data leak). This is reinforced by Section 168 of the DPA 2018. The following court rulings are examples of how these guidelines are enforced in practice, focusing specifically on instances where non-compliance with the duty of care has occurred:

ICO v British Airways (2020): The Information Commissioner's Office (ICO) punished British Airways with a fine of £20 million for not having Multi-Factor Authentication (MFA) and for having weak Security Information and Event Management (SIEM) systems. The attack, which was the result of an unpatched vulnerability, led to the breach of personal data of about 400,000 customers, including credit-card information and other highly confidential personal data.[15]

ICO v Marriott International (2020), The ICO imposed an enormous fine of £18.4 million on Marriott for their inefficient network segmentation and lack of monitoring. As a result, a breach that originally took place in Starwood's systems back in 2014 remained undetected until 2018, despite Marriott's acquisition in 2016. During this time, the personal data of about 339 million worldwide guests – names, addresses, passport numbers, etc. – had already been compromised.[16]

Various Claimants v WM Morrison Supermarkets plc [2020] UKSC 12The UK Supreme Court ultimately cleared Morrisons of vicarious liability for a malicious data breach carried out by a disgruntled employee who deliberately posted payroll data online. While the company escaped liability on those facts, the judgment (especially per Lord Reed) underscored how critical it is to keep tight access controls in place. The Court made clear that giving staff broader permissions than they actually need for their jobs can itself amount to organisational negligence – a point that has since become required reading for anyone designing "least-privilege" policies.[17]

TalkTalk Telecom Group (2016), In what was, at the time, the ICO's largest-ever fine under the old Data Protection Act 1998 regime, TalkTalk was penalised £400,000 for a catalogue of basic security failures. Outdated and

[15] *Various Claimants v Wm Morrison Supermarkets plc* [2020] UKSC 12 [2020] AC 989.
[16] *ICO v TalkTalk Telecom Group plc* [2016] (ICO Penalty Notice).
[17] National Cyber Security Centre (NCSC), 'Cyber Essentials: Requirements for IT Infrastructure' (2018).

unpatched web-server software, combined with inadequate encryption of sensitive customer data, left a glaring SQL-injection vulnerability wide open. A relatively unsophisticated attacker exploited it in October 2015, gaining access to the personal and financial details of 157,000 customers – including names, addresses, dates of birth, and, in thousands of cases, bank account numbers and sort codes. The case remains a textbook example of how neglect of routine patching and poor data-handling practices can trigger both regulatory sanctions and lasting reputational damage.[18]

Taken together, these cases drive home a point that no data controller can afford to ignore: serious compliance with the security obligations in the UK GDPR and the Data Protection Act 2018 is not optional.

If companies regard encryption, patching, access controls, and monitoring as mere box-ticking exercises (or even worse, completely ignore them), the outcome is almost always huge regulatory fines, personal injury claims worth millions of pounds and the company's reputation suffering in the long run. In the cases involving the firms Marriott, TalkTalk, and Morrisons, the litigation has largely shown how the bar has been set higher by the courts and the regulators to ensure that firms are improving their systems of security on an ongoing and proactive basis, rather than in a purely reactive manner after the event has occurred. In an environment in which threats are changing at an ever-accelerating pace, the message could not be clearer: invest in the security of the business, and do it properly, or pay the price down the line in terms of money and reputation.

The Cyber Essentials program that was developed and is now managed by the National Cyber Security Centre (NCSC) not only provides a solid foundation for legal obligations but also highlights them through five very simple but essential technical controls: boundary firewalls, secure user access controls, timely software patching, effective malware protection, and systematic vulnerability management. For small and medium-sized enterprises in particular, the scheme has come to serve as a highly practical, accessible benchmark – one that allows organisations to demonstrate, in a way regulators and courts readily recognise, that they are meeting the "appropriate technical and organisational measures" demanded by the UK GDPR.[19]

2.2. The Civil Wrongs Ordinance and the Draft Data Protection Law of 2025.

The amended British Civil Wrongs Ordinance No. (5) of 1947, effective in the West Bank, particularly its Article 50, forms the legal basis for civil liability for damages resulting from negligence. Negligence, in essence, is nothing more than causing harm through a lack or absence of due care.[20] According to Article 50 of the Civil Wrongs Ordinance, negligence consists of:

---

[18] S Al-Sayigh, *Civil Wrongs (Tortious Liability)* (1st edn, Al-Bahr and Al-Hay'ah Al-Khayriyah Press 1997) [Arabic].

[19] S Khan, C Roberts 'Operationalising Article 32 UK GDPR: The Role of Cyber Essentials as a Compliance Bridge for UK SMEs in a Post-Brexit Regulatory Landscape' (2024) 137 Computers & Security 103629. DOI: https://doi.org/10.1016/j.cose.2023.103629.

[20] B Cinar, *Supply Chain Cybersecurity: Legal and Technical Perspectives* (Cybersecurity Press 2023) 78.

"(a) doing an act which a person of ordinary prudence and foresight, in the circumstances in which the act was done, would not do, or omitting to do an act which such a person would not omit to do in the circumstances in which the omission took place;
(b) or omitting to use the skill or take the care which, in the circumstances, a person of ordinary prudence and foresight, possessing that skill, would use or take in that profession, trade, or art.
In respect of another person to whom the person who did the act or omitted to do it or to use the skill or take the care as aforesaid, owes a duty not to do that act, or to omit to do it, or to use the skill or take the care, as the case may be..."

This publication is a must for organizations to take actions that could prevent predictable damage, based on the "reasonable person standard", which denotes the behavior that society expects a reasonable entity in similar situations to display. In the context of cybersecurity, this standard is used to determine whether the security measures taken by organizations to prevent cyber-attacks are sufficient or not.[21]

The confirmation comes from the stipulations of Article 55 bis (a) of the revised British Civil Wrongs Ordinance of 1947, which declare: "...the infringement of a legal obligation is the non-fulfillment of any person's obligation imposed by any law, other than this Ordinance, if the actual aim of that law, after its true interpretation, is to give or protect another person, and the other person suffers the type or kind of loss that was meant to be prevented by that law through the non-fulfillment..."

The article referred to above implies that statutory duty breach happens if a person does not perform a task required by the law, as long as that law is meant for the protection or advantage of another party. This necessitates the proper understanding of the legislation's intent in order to figure out whether it really is intended to protect a certain group of people, and that the damage being suffered is of the kind that the legislation is trying to prevent. To illustrate, if a specific law requires safety equipment to be provided by the employer and the worker gets hurt due to the lack of it, this non-delivery will be considered a statutory duty breach and will lead to civil liability.

This provision establishes a clear pathway for imposing civil liability on individuals or organisations whose failure to comply with statutory obligations causes harm. At its core, it requires courts to examine two critical issues: whether the legislation was specifically intended to prevent the type of damage that occurred, and whether the harm suffered falls within the scope of protection the statute was designed to afford. In practice, successful claims hinge on demonstrating this close nexus between legislative purpose and actual injury, a principle that has long ensured the article serves as an effective tool for safeguarding the very groups Parliament sought to protect. This approach reinforces the principle of liability in the Civil Wrongs Ordinance, where breach is assessed based on objective standards linking duty, damage, and legislative purpose.

The Draft Data Protection Law of 2025 is intended to create an advanced statutory scheme to improve Cybersecurity and the protection of Personal

[21] A Abu Haniyeh, *Cybersecurity Strategy and Its Indicators* (National Protection Center for Cybersecurity 2023) [Arabic].

Data. Core obligations contained in the Draft Data Protection Law will protect the rights of individuals and require compliance through the following:

Authorising the National Data Protection Authority to set classification level security standards, such as the use of Encryption Technology, to provide periodic Risk Assessments.

Requiring Data Controllers to take reasonable and proportionate steps in developing security measures to mitigate and reduce the likelihood of any Security Breaches at acceptable levels. As examples, measures such as AES-256 Encryption, Multi-Factor Authentication and the implementation of Intrusion Detection Systems would be included within this requirement.

Establishing a 72-hour time frame to notify the National Data Protection Authority and/or affected individuals whenever a Cyber Incident is likely to result in a threat to the Rights and Freedoms of individuals.

Establishing a civil liability regime that creates a framework by which individuals may receive it for their Harm caused by insufficient Data Protection, including to recoup the Material Losses (by Fraud and/or Identity Theft) and Non-Material Losses (by Damaging an Individual's Reputation and Trust).

The Draft Data Protection Law will establish that there may be Administrative Fines, which would act as a deterrent to assist in the enforcement and ensure compliance with the Draft Data Protection Law.

In 2025, the Palestinian Authority has proposed a Data Protection Act which demonstrates their commitment to creating a safe digital environment through its emphasis on being clear and open, responsible and accountable, and to providing a proper level of security for both users and their data to build trust in digital services.

That said, one notable departure from more mature regimes (most obviously the UK GDPR) is the absence of an express right to compensation for non-material damage. Psychological distress, reputational harm, or the intangible loss of trust following a breach – losses that UK and EU courts now routinely recognise and award damages for – are not currently covered. This omission narrows the remedial landscape considerably and, in practice, places the Palestinian framework at a more restrained level of liability than its Western counterparts

The Palestinian Data Protection Law, as a new law, faces significant challenges in its practical application, including:

- Lack of technical expertise: In order to prove the breach of the duty of care, digital forensic reports are needed to ascertain the causes of the breach and the level of negligence. Palestine, however, faces a lack of resources in this area, [22] hindering accurate technical investigations.[23]
- Absence of judicial precedents: The Palestinian judicial system does not have clear judicial rulings that set standards of reasonableness and foreseeability of damage in the context of cybersecurity, which

[22] Kosseff (n 5) 145–147.

[23] International Organization for Standardization (ISO), 'ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements' (2013).

according to some, results in general judicial interpretations that might not be precise. [24]

- Absence of unified local security standards: Unlike international standards such as ISO/IEC 27001 or the British Cyber Essentials program me, there are no unified local security standards in Palestine, [25] making it difficult to determine what constitutes "reasonable" security measures.[26]
- Involvement of third parties: Cyber-attacks often involve external parties, such as hackers or malware, complicating the proof of foreseeable damage or liability. For example, the Home Depot case (2014) in the United States showed the difficulty of holding organisations liable when attacks are caused by sophisticated external parties.[27]
- Full Israeli control over internet infrastructure, including control over the import of technical equipment and restrictions on the development of local networks.[28]

In a hypothetical scenario, if a Palestinian bank neglected to implement Multi-Factor Authentication (MFA), leading to a leak of customer data, affected individuals could claim compensation under Article 24 of the Draft Data Protection Law, relying on Article 50 of the Civil Wrongs Ordinance to prove negligence. [29] However, proving negligence requires presenting precise technical evidence, such as digital forensics reports, highlighting the need to develop technical and judicial capabilities. [30] The National Data Protection Authority could also impose fines under Article 33, but the effectiveness of these penalties depends on the Authority's ability to conduct accurate and transparent technical and legal investigations. [31] The mentioned challenges, such as the lack of technical expertise and local standards, confirm the need for investments in technical infrastructure and training, [32] alongside the development of clear judicial precedents to enhance the effectiveness of the Draft Data Protection Law 2025 and ensure better protection of personal data in Palestine.[33]

2.3. Special Conditions for Considering an Act a Civil Wrong in the Context of Personal Data Protection.

Not Constituting a Conflicting Claim with the Repetition of the Act:

This part requires that the act not be of a type whose repetition leads to repeated or unjustified legal disputes. In the context of personal data protection, this condition can be applied to cases such as a company's database

[24] Cinar (n 20) 85.
[25] D J Solove, W Hartzog, *Breached! Why Data Security Law Fails and How to Improve It* (OUP 2022) 112–115.
[26] F Amoretti and others, 'Palestine: Whose Cyber Security Without Cyber Sovereignty?' in SN Romaniuk and M Manjikian (eds), *The Routledge Companion to Global Cyber-Security.*
[27] sup *Strategy* (Routledge 2021).
[28] Palestinian Draft Data Protection Law 2025, art 24.
[29] Kosseff (n 5) 149.
[30] Palestinian Draft Data Protection Law 2025, art 33; Cinar (n 20) 94.
[31] Kosseff (n 5) 149.
[32] Cinar (n 20) 94.
[33] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311.

breach due to negligence in securing data. If the breach leads to the theft of customer data (such as credit card numbers or personal information) and causes substantial harm like financial fraud, this act is considered a civil wrong because it causes specific damage and is not merely a repetition of trivial disputes. For example, the case of Vidal-Hall v Google Inc [2015] EWCA Civ 311 in English law recognised that the misuse of personal data can constitute a privacy breach worthy of compensation.[34] If the act relates to the leakage of non-sensitive data (like a general email address) without tangible harm, it might be excluded as it could be interpreted as part of recurring digital interactions that do not form the basis for a legal claim, preventing it from becoming a conflicting claim.

Improbability of the Act Being Committed by a Person of Ordinary Perception and Temperament:

This condition requires the act to be serious enough to motivate an ordinary person to file a complaint under the surrounding circumstances, based on the "reasonable person standard" derived from English common law, as in the case of Blyth v Birmingham Waterworks Co (1856) 11 Ex 781, which defined negligence as the omission to take the care a prudent person would take.[35]

Due to the potential impact on individuals whose highly sensitive personal information (such as medical records or banking information) has been improperly disclosed, as a result of a technology company not exercising due diligence and care, there is a clear basis for establishing this type of conduct as a civil wrong. This includes not only the creation of financial harm (direct losses) but also the psychological harm (anxiety and distress) that can ensue from the improper release of highly sensitive personal information. Furthermore, it is reasonable to expect that organisations that are entrusted with personal data will ensure an acceptable level of security in order to safeguard those data. This expectation is well established and ingrained in our society today.[36]

The UK Supreme Court's decision in Lloyd v Google LLC[37] is a definitive confirmation that compensation under Article 82 is not automatic. While the representative action failed, the Court did make clear what the evidentiary standard is for recovering damages, the UK Supreme Court confirmed that the mere violation of a person's rights under data protection legislation (and proven psychological harm) can provide a basis for compensation. Therefore, the judgment adds weight to the broader notion that non-material damages are no longer considered secondary (or peripheral) to this area of the law, but rather are now an integral aspect of the remedial framework.[38] By contrast, when the violation is genuinely trivial (say, sending a few unsolicited marketing emails with no real harm done), courts tend to treat it as something we simply have to live with in the digital age. After all, commercial spam has become part of the furniture of online life, and the threshold of tolerable inconvenience is set far higher than, for instance, the unauthorised disclosure of medical or

[34] *Blyth v Birmingham Waterworks Co* (1856) 11 Ex 781.
[35] *Lloyd v Google LLC* [2021] UKSC 50.
[36] J Pool and others, 'A systematic analysis of failures in protecting personal health data: A scoping review' (2024) 74 Int J Inf Manag 102719 <https://doi.org/10.1016/j.ijinfomgt.2023.10271>.
[37] Lloyd (n 36)
[38] N Nour, 'Damages: Restitutio in Integrum' in Fernández Antuña Antolín (ed), *Jus Mundi* (29 August 2025).

financial records. In such cases, the conduct rarely crosses the line into what would properly be regarded as an actionable civil wrong.

3. The Element of Damage in Cyber Liability Cases (From Tangible to Intangible Damages).

Article 1 of the British Civil Wrongs Ordinance of 1944 defines the term "damage" thus: "loss or injury to property, or deprivation of comfort, or injury to physical well-being or reputation, etc." Damage, as a notion, is one of the key aspects in civil liability cases related to cyber breaches, reflecting the very essence of compensatory claims in the context of intrusion, data leaks, or breach of privacy. The assessment of compensable damage in cases related to cyber liability is not always easy to establish, not only because it is necessary to determine whether the damage is financial, related to fraud or clean-up costs, or moral, reflecting the plaintiff's state of mind, but also to satisfy the quantification requirements, which differ significantly across the globe. The following chapter will attempt to provide a comparative overview regarding the assessment, proof, and compensability of damage in data protection cases, referring to two sets of laws, which, despite their significant differences, will be used to provide the reader with a better understanding of the issue, namely the mature, but now post-GDPR regime in the UK, and the emerging regime currently under development in Palestine. The discussion will be divided into two parts, the first referring to the assessment of material damage, where the routes for recovering financial loss are relatively well established under the laws of the UK and Palestine, while the second part will address the more complex issue of moral damages, where the Palestinian regime is lagging far behind the generous standards currently firmly established in the case law of the UK and the EU.

3.1. Material (Tangible) Damage in Cyber Liability Cases.

Material damage is defined as measurable financial loss resulting from cyber breaches, such as costs for system restoration, credit monitoring, ransom payments, or loss of profits. Proving it requires precise financial documentation, such as invoices or expert reports, to ensure compensation according to the principle of *restitutio in integrum*, i.e., restoring the affected party to their position before the damage occurred.[39] This section discusses material damage in British and Palestinian legal systems.

Firstly: Material Damage in British Law - Legal Framework.
In the United Kingdom, material damage in cyber liability cases is regulated by a legal framework combining the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR), and common law principles. Under Article 82 of the UK GDPR, any individual who suffers material or non-material damage as a result of a data breach due to non-compliance with the

[39] UK GDPR (n 14) art 82.

Regulation is entitled to claim compensation from the controller or processor.[40]

Material damage in this context typically takes three main forms: the direct costs of restoring systems compromised or destroyed in a cyber-attack; the often-substantial expenses individuals incur for credit-monitoring services and identity-theft protection in the aftermath of a breach; and, most seriously, the financial losses flowing from actual identity theft or fraud enabled by the leaked data. [41]

This private right of action runs alongside, and is entirely independent of, the regulatory enforcement powers of the Information Commissioner's Office (ICO). In practice, it enables affected data subjects to bring civil claims on their own initiative and recover compensation even when the ICO chooses not to pursue (or has not yet completed) its own investigation. [42]

In Lloyd v Google LLC [2021] UKSC 50 the UK Supreme Court settled a point that had caused considerable uncertainty: compensation under Article 82 UK GDPR is never automatic. A claimant must prove actual damage – whether material or non-material – and the mere fact that a breach has occurred, however serious the infringement of the regulation may be, is not enough on its own.Material damage in this context most commonly takes the form of out-of-pocket expenses: the cost of forensic recovery or system rebuilding after an attack, losses directly attributable to fraud or identity theft, credit-monitoring subscriptions taken out in response to the breach notifications, and reasonable legal or administrative costs incurred in mitigating the consequences of the incident.

When awarding compensation, courts are bound by the classic principle of restitutio in integrum: the claimant should, as far as money can do it, be placed in the same financial and psychological position they enjoyed before the wrongful act occurred – no more, no less.[43]

In the specific context of cyber-liability claims, this principle finds direct expression in Article 82 of the UK GDPR. That provision explicitly permits recovery of both material damage (the cost of system restoration, credit-monitoring subscriptions, fraud losses) and non-material damage (serious distress or reputational injury).[44]

Thus, if an individual suffers concrete financial loss because fraudsters exploited data released in a breach, the court will aim to make good that loss pound for pound; the aim is neither to punish the defendant nor to leave the victim short-changed, but simply to restore the status quo ante. [45]

This is evident in the case of Warren v DSG Retail Ltd,[46] where Saini J refused the claimant's claim for the cost of credit monitoring services on the basis that no invoices, receipts, or other tangible evidence of outlay had been placed before the court. It is clear that the court will not pay compensation, even in

[4040] Information Commissioner's Office (ICO), 'Guide to the GDPR: Right to Compensation' (2025).
[41] *Lloyd* (n 39).
[42] F Cuena Boy, 'Restitutio in integrum (DCH)' (Max Planck Institute for Legal History and Legal Theory Research Paper Series No 2024-10, 2024).
[43] UK GDPR (n 14) art 82.
[44] DPA 2018 (n 43) s 168.
[45] *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB).
[46] ibid.

data breach claims, on a speculative basis.: there must be hard proof of loss actually suffered. Absent such evidence, the claimant cannot be restored to the position they occupied before the breach, and the claim therefore fails. The case has quickly become authoritative on the point that accurate, contemporaneous documentation of loss remains indispensable if Article 82 GDPR damages are to be recovered in practice.[47]

Secondly: Material Damage in American Law - Legal Framework. In the United States, material damage from cyber breaches covers direct financial losses (system repair, forensic costs) and indirect losses (lost profits, missed business opportunities). Tort law governs compensatory damages, while statutes like the California Consumer Privacy Act (CCPA) and the CLOUD Act allows statutory damages of $100–$750 per consumer per incident (or actual losses if higher) and, for intentional violations, civil penalties up to $7,500 per breach.[48]

In In re Equifax, Inc Customer Data Security Breach Litigation,[49] the court held Equifax liable for the 2017 data breach that exposed the personal information of approximately 147 million people. The ruling was based on the legal duty of care stipulated in the Gramm-Leach-Bliley Act (15 U.S.C. § 6801(b); 16 C.F.R. § 314.3), which obliges financial institutions to protect customer data, and on Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45(a)), which prohibits unfair practices that cause substantial harm to consumers

In the case of In re Equifax, Inc. Customer Data Security Breach Litigation,[50] the court dealt with the data breach that occurred in 2017, which revealed the personal data of about 147 million people. The court held Equifax liable for not following the federal statutory obligations regarding the protection of consumer financial information and the prohibition of unfair trade practices.[51] The $425 million settlement remains a landmark in U.S. data-breach litigation.[52]

The court further anchored Equifax's liability in the classic tort principle of foreseeability. Evidence showed that the company had received clear, public warnings about a critical vulnerability in the Apache Struts software as early as March 2017, yet failed to apply the available patch in a timely manner. In the court's view, a breach of this magnitude was not merely possible but entirely foreseeable; the failure to act on known, high-risk vulnerabilities therefore constituted a clear breach of the reasonable standard of care expected of a major credit-reporting agency. The court also relied on the precedent Collins v Athens Orthopedic Clinic 307 Ga 555 (2019). to affirm that the mere exposure of personal data to hacking constitutes a legal injury because it opens the door to risks of identity theft, and the occurrence of subsequent financial fraud is evidence of direct causality, which established Equifax's liability for the resulting damages.[53]

---

[47] California Consumer Privacy Act 2018, Cal Civ Code § 1798.150.
[48] Gramm-Leach-Bliley Act 1999, 15 USC § 6801(b); 16 CFR § 314.3; Federal Trade Commission Act 1914, 15 USC § 45(a).
[49] In re Equifax, Inc Customer Data Security Breach Litigation (MDL No 2800, ND Ga 2022).
[50] ibid.
[51] Gramm-Leach-Bliley Act 15 USC § 6801(b); 16 CFR § 314.3; Federal Trade Commission Act 15 USC § 45(a).
[52] *Collins v Athens Orthopedic Clinic PA*, 307 Ga 555 (2019).
[53] *In re Anthem, Inc. Data Breach Litigation*, No. 15-md-02617-LHK (ND Cal, 2018).

American law, through its recent decisions in the field of data breaches, provides a good principle based on the recognition of the civil liability of companies resulting from the infringement of the legal duty to keep personal data in their custody secure. The case of Anthem may be considered the most evident example of the willingness of American judges to consider a data breach as, by itself, a prima-facie case of unreasonable security practices. The district court did not dismiss the case at the pleadings phase, holding that the mere fact of the successful data breach of 79 million individuals was sufficient to sustain a reasonable inference of unreasonable practices in data security, as implied by tort law and the company's own privacy policy. However, most importantly, the liability was not limited to actual out-of-pocket loss. The final settlement approved in 2020 covered actual financial loss, but it also covered substantial awards for time expended on mitigation, credit monitoring, and, in a marked departure from the traditional scope of tortious liability under the common law, a figure for the inherent loss of privacy in the form of the increased likelihood of identity theft in the future. The message of the Anthem litigation has become a landmark statement of the proposition that the liability for data breach can, and increasingly does, extend beyond economic loss to embrace the concepts of moral injury and potential risk, thereby providing the consumer with a much broader framework of potential redress than many civil law systems would currently support. [54]

Most importantly, however, liability was not restricted to actual out-of-pocket damages. The settlement that was finally approved in 2020 will provide for compensation for actual financial losses, but will also include significant awards for time expended in mitigation, for credit monitoring services, and, in a dramatic shift away from traditional notions of the boundaries of tort liability, for an element recognizing the increased risk of future identity theft and the inherent damage to privacy. In other words, the court and the parties were effectively recognizing that the damage to the value of personal information and the non-economic damage resulting from a data breach are, in and of themselves, compensable forms of damage. The Anthem case has thus become a landmark authority for the proposition that data breach liability does, and increasingly will, go beyond actual economic damage to encompass moral damage and future risk, thus providing a potentially much broader framework." Most importantly, [55] however, liability was not restricted to actual out-of-pocket damages. The settlement that was finally approved in 2020 will provide for compensation for actual financial losses, but will also include significant awards for time expended in mitigation, for credit monitoring services, and, in a dramatic shift away from traditional notions of the boundaries of tort liability, for an element recognizing the increased risk of future identity theft and the inherent damage to privacy. In other words, the court and the parties were effectively recognizing that the damage to the value of personal information and the non-economic damage resulting from a data breach are, in and of themselves, compensable forms of damage. [56] The Anthem case has thus

[54] ibid.
[55] Federal Rules of Civil Procedure, r 23.
[56] *TransUnion LLC v Ramirez*, 141 S Ct 2190 (2021); *Tsao v Captiva Software Inc*, 2020 US Dist LEXIS 172113 (SD Fla).

become a landmark authority for the proposition that data breach liability does, and increasingly will, go beyond actual economic damage to encompass moral damage and future risk, thus providing a potentially much broader framework of remedies for the consumer than many civil law traditions might support.[57]

Thirdly: Material Damage in Palestinian Law. In Palestine, material damage is defined under the Civil Wrongs Ordinance (1944) as "the term 'damage' means loss or injury to property, or deprivation of comfort, or injury to physical well-being or reputation, etc." (Article 2). In the context of cyber liability, this includes costs for system restoration, ransom payments, or compensating customers for financial losses. Article 3 obligates the causer to compensate, stating: "The following matters, as set out in this Ordinance, are civil wrongs, and subject to the provisions of this Ordinance, any person who has suffered harm or damage, due to a civil wrong committed in Palestine, is entitled to obtain the redress which this Ordinance grants him from the person who committed that wrong, or who is responsible for it... Provided that no act shall be deemed a civil wrong if its repetition would not lead to the formation of a conflicting claim, and would not cause a person of ordinary perception and temperament to complain under the circumstances surrounding the case."

The aforementioned article sets the framework for tortious liability by granting a person who has suffered harm or damage within Palestine the right to seek "redress" (compensation or legal remedy) from the perpetrator or person responsible for the civil wrong. The claimant must still prove both damage and a causal link, requirements that remain firmly rooted in the English common-law tradition, most famously articulated in Donoghue v Stevenson [1932] AC 562, the case that gave us the modern concept of duty of care. [58]

In relation to the particular sector of personal data protection, Article 3 is easily employed within the two broad themes of illegal conduct, namely the negligent handling of private data (failing to protect databases, lack of controls on access, inter alia), as well as intentional breaches (unauthorised publication/discovery of private information). If harm, whether of a tangible (loss from financial fraud, clean-up expenses) or non-material (clinically significant distress, defamation, inter alia) nature, is thereby caused, it is clearly a civil wrong. The article thus expands the traditional tortious regime into the new arena of cyberspace, while ensuring that the essence of causation is retained, with a corresponding modification of 'breach' to suit the peculiarity of the handling of private data.

The goal is to achieve justice by compensating the affected party, considering the modern technological context.

Referring to the rulings of Palestinian courts, we find that they have not directly addressed cyber liability cases, but principles can be extrapolated from the following rulings:

The Palestinian Court of Cassation, Decision No 11/2024 (14 May 2024) held that: Material damage in tortious liability requires proving actual or anticipated financial loss (such as burial expenses or loss of support) with clear evidence proving its occurrence and its causal link to the harmful act. Speculative or

[57] Tsao v Captiva MVP Restaurant Partners LLC 986 F3d 1332 (11th Cir 2021).
[58] *Ramirez* (n 57).

unsubstantiated claims are rejected, and the damage must be personal to the claimant, according to Article 55/1/7 of the Civil Wrongs Ordinance of 1944.

In the same context, Palestinian Court of Cassation, Decision No 453/2022 (10 December 2023)., held that material damage, as defined by Article 1 of the Civil Wrongs Ordinance No. 36 of 1944, is the actual loss or expense estimable in monetary terms. For a compensation ruling, the plaintiff must detail it in the statement of claim or its attachments, negating gross uncertainty according to Article 60(b). The statement must contain the act of damage, the dates of the act of damage, and the nature of the material damages for the case to be considered acceptable, with the emphasis being that a defect in the details of the statement does not necessarily disqualify the case, as upheld by the Court of Cassation Ruling No. 847 of 2020.

The judgment also clearly distinguishes between the grounds of objection to the case, whether substantive or procedural, as in the case of a denial of the case being vexatious. The judgment clearly states that an inadmissibility plea under Article 90 of the Code of Civil and Commercial Procedure may only be grounded on purely procedural grounds. It follows then that where the plaintiff has furnished the court with the requisite particulars of the act of damage, it becomes unlawful for the court to strike the case off for uncertainty. The court must then proceed to examine the case to determine the extent of the loss. Anything less than this would be a violation of the principle of procedural economy and the plaintiff's constitutional right to have the case heard by the trial court.

In my view, the UK takes a fair stance on proving damage and standing in cyber liability cases under Article 82 of the UK GDPR, which requires proof of actual damage, whether material or non-material. This is substantiated by the ruling in Lloyd v Google LLC [2021] UKSC 50, which reiterated that a simple data breach is insufficient for a claim of compensation, which requires proven financial loss or psychological suffering, signifying a dedication to judicial specificity. However, it is significant that the UK stance is far more sympathetic to claims of psychological suffering than the United States. Where American courts (outside a scattering of progressive states) remain loath to commit to a full compensation remit unless there is actual physical harm or, at the very least, some form of pecuniary loss, the UK has clearly gone the other way.[59]

This is clearly demonstrated in the case of Warren v DSG Retail Ltd [2021] EWHC 2168 (QB). In that case, although the claim failed, it is significant that it failed not on the basis that a lack of financial loss following a data breach, amounting merely to anxiety/distress, is automatically non-compensable. Instead, Mr. Justice Saini simply stated that he rejected the case on a narrow technical point that the plaintiff could not plead a degree of distress sufficient to cross the threshold for compensation. In short, the court clearly indicated that, but for the lack of severe psychological damage, compensation would be available even in the absence of even a single penny of economic loss.[60]

[59] 'Liability for nonmaterial damage under the GDPR: Approaches of EU, UK courts' (IAPP, 13 December 2025) <https://iapp.org/news/a/liability-for-non-material-damage-under-the-gdpr-approaches-of-eu-uk-courts>.

[60] UK High Court dismisses claims following DSG data breach' (Lexology, 5 August 2021) <https://www.lexology.com/library/detail.aspx?g=f6664c7c-fa39-4320-8bfd-609b4b776f38> accessed 13 December 2025.

a far more stringent bar is adopted within the American jurisprudence. There,Cyber-breach plaintiffs are required to show that they alleged an actual or threatened "injury in fact" to plead standing, particularly within a class action suit. In the Supreme Court's opinion in TransUnion LLC v Ramirez (2021), a plaintiff's allegation that his identity might be stolen, together with a claims defendant's insistently inaccurate storage of his particular private information, lacked sufficient immediacy to state a valid claim seeking relief in compensation. Such a plaintiff's threat of identity theft, especially with thus-far unfrozen private data, is insufficient to state a valid claim when suffering no contemporaneous financial harm. This stringent approach is far more restrictive when contrasted with the current, far more permissive regime adopted within the U.K.[61]

On the other hand, the American rule is far more stringent. It has been emphasized that to develop standing, especially in a class action suit, it is necessary that there be an actual or imminent "injury in fact." The Supreme Court, in the case of TransUnion LLC v. Ramirez (2021), has ruled that a possible threat of identity theft or improper storage of data cannot constitute a grievance eligible for compensation unless there is some concrete, immediate harm involved. This is a far more restrictive regime on cyber breaches that result in no real, immediate, or pecuniary harm, as is now recognized under UK law. [62]

As for Palestinian law, it is the most flexible, as detailing material or anticipated damage (such as loss of profits or reputation) is sufficient without requiring imminent harm, as evident from Palestinian Court of Cassation decisions, like Decision 453/2022 (10/12/2023). This flexibility, derived from the Civil Wrongs Ordinance of 1944, allows affected parties to file lawsuits based on potential losses. The absence of punitive damages makes the scope narrower compared to the American system, which may reduce its effectiveness in deterring gross negligence, a topic which will be discussed in the second section.

3.2. Moral Damage in Cyber Breaches.

Moral damage is the non-material harm that affects an individual's dignity, feelings, reputation, or social standing, and is characterised by difficulty in estimation compared to material damage measurable financially, such as costs for replacing credit cards or credit monitoring. [63] It includes psychological distress, emotional pain, anxiety, social embarrassment, or harm to reputation resulting from the violation of personal rights like privacy or honour.[64] In the context of cyber breaches, moral (non-material) damage primarily stems from

---

[61] TransUnion LLC v Ramirez 594 US 413 (2021) (Supreme Court of the United States) <https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf> accessed 13 December 2025.

[62] MSM Alqudah, 'Civil Legal Framework for Moral Damage in Jordanian Law' (2024) 16 Pakistan Journal of Criminology 317.

[63] WH van Boom, 'European Tort Law – An Integrated or Compartmentalized Approach?' in A Vaquer (ed), *European Private Law Beyond the Common Frame of Reference* (Europa Law Publishing 2008).

[64] Abdelaziz Al-Sasmeh, *Tortious Civil Liability, The Harmful Act* (Al-Dar Al-Ilmiyah Al-Dawliyah and Dar Al-Thaqafa 2002) 90 [Arabic], D J Solove, *The Digital Person: Technology and Privacy in the Information Age* (NYU Press 2004) 45.

the unauthorised disclosure or misuse of personal data, producing tangible psychological and social consequences for the victim: persistent anxiety over potential identity theft, constant fear of blackmail following the leak of intimate photographs or medical records, or a profound sense of helplessness and personal violation when one's financial or health history becomes accessible to strangers.

These effects are far from mere transient embarrassment. In many cases they evolve into genuine psychiatric disorders (generalised anxiety, depression, or even post-traumatic stress disorder in severe instances) and can endure for years and significantly impair quality of life and interpersonal relationships. Consequently, moral damage in data-breach litigation must be regarded as real and compensable harm in its own right, even in the complete absence of direct financial loss. [65]

A growing body of jurisprudence (particularly in post-GDPR Europe) now recognises that the very fact of a serious cyber breach constitutes a profound assault on personal privacy. Victims frequently describe an overwhelming sense of helplessness, a lasting erosion of trust in the institutions entrusted with their data, and, in many cases, acute social embarrassment that can linger for years. [66]

The harm becomes especially intractable when the breach involves the publication of intimate photographs or deeply private records. Reputational injury of this kind is often effectively irreversible: even successful takedown efforts rarely erase every trace from the internet, leaving the individual with a permanent digital shadow. [67]

What sets moral damage in cyber cases apart from traditional torts is its inherently transnational and intangible character. Unlike a cross-border, digital phenomenon that is far harder to quantify and prove than, say, a broken limb. Courts are therefore grappling with the challenge of translating subjective, non-pecuniary suffering into compensable loss without the comfort of concrete medical bills or lost earnings statements, a task that remains one of the most difficult frontiers in contemporary privacy litigation. [68]

Legal systems differ in addressing moral damage. In British law, Article 82 of the GDPR allows compensation for non-material damage without proving financial loss.[69] In Various Claimants v WM Morrison Supermarkets Plc [2020] UKSC 12, the UK Supreme Court affirmed the company's liability for the psychological distress of 100,000 employees due to a data leak by an internal employee.[70] In American law, proof of tangible psychological harm is required. In compensation for general anxiety was rejected due to the lack of medical evidence.[71] In In re Anthem, Inc Data Breach Litigation 327 FRD 299 (ND Cal 2018) compensation was only accepted for those who provided medical reports proving psychological impact.[72]

---

[65] ibid 47.
[66] ibid 49.
[67] Rogers (n 58) 127.
[68] Regulation (EU) 2016/679 (GDPR), art 82.
[69] *Various Claimants* (n 19).
[70] *In re Yahoo! Inc Customer Data Security Breach Litigation*, 334 F Supp 3d 1010 (ND Cal 2019).
[71] *In re Anthem* (n 52).
[72] Civil Wrongs Ordinance 1944, art 2.

In Palestinian law, moral damage is defined under Article 2 of the Civil Wrongs Ordinance (1944) as an infringement on honour or reputation,[73] but it faces challenges in the cyber context due to the absence of specialised judicial precedents. [74] Palestinian Court of Appeal, Appeals Nos 819/2022 and 900/2022 (30 June 2024), the court confirmed that moral damage is limited to infringement on reputation or honour and does not include general psychological distress without strong evidence. [75] The Palestinian Court of Cassation, Decision No 632/2025 (13 February 2025).that compensation for moral damage requires an explicit legal text, and pure moral damage is difficult to estimate without primary evidence, and in this case, the plaintiff did not prove moral damage, so the failure to award moral compensation was in accordance with the law.[76]

4. Legal Integration Between Articles 60 and 55 bis in Addressing Causality.

Proving causality is an essential element in civil liability cases for cyber breaches, requiring the determination of the direct or contributory link between negligence or the wrongful act and the resulting damage. This issue gains special importance in the context of cyber breaches due to the complexity of intertwined causes, such as negligence by entities responsible for data protection, actions of hackers, or even negligence by the victims themselves (e.g., using weak passwords). This chapter discusses the legal integration between Article 60 and Article 55 bis of the effective British Civil Wrongs Ordinance in Palestine, with reference to Article 50, to analyse how causality is addressed in cyber liability cases.

4.1. Article 60 of the Palestinian Civil Wrongs Ordinance Provides a Solid Legal Framework for Linking Compensation to Causality.

Article 60 of the British Civil Wrongs Ordinance of 1944 states: "Compensation may be awarded either alone or in addition to a prohibitory or mandatory order, subject to the following conditions:

(a) If the plaintiff has suffered damage, punishment shall only be for damage which might naturally arise in the ordinary course of things and which directly results from the civil wrong committed by the defendant.

(b) If the plaintiff has suffered material damage, compensation for that damage shall only be awarded if the plaintiff has detailed that damage in his statement of claim or attached it thereto."

Article 60 of the British Civil Wrongs Ordinance links compensation to causality by requiring direct or foreseeable damage (clause a) and detailing material damage (clause b).

[73] Civil Wrongs Ordinance 1944, art 64.
[74] Appeal Nos 819/2022 & 900/2022 (Palestinian Court, 30 June 2024).
[75] Court of Cassation Decision No 632/2924 (13 February 2025).
[76]CrowdStrike, 'Log Files: Definition, Types, and Importance' (20 December 2022).

Article 60 of the Civil Wrongs Ordinance (which remains in force in Palestine) is heavily weighted towards pecuniary loss. Subsection (b) of Article 60 does so explicitly by requiring "the claimant to particularise the loss in his statement of claim." Such a phrase seems to marginalise claims of non-pecuniary loss. In an age where cybercrime causes severe emotional distress, loss of privacy, and anxiety, it seems to offer victims no hope of recompense for what most directly concerns them. The Equifax settlement in the US in 2017, which involved substantial damages claims for "emotional distress" due to identity theft, represents what Article 60 currently has no possibility of awarding. [77]

The same provision (b) also sets an almost insurmountable evidentiary bar for the digital case. The demand for "precise details" of the damage forces the plaintiff to submit advanced technical evidence – system logs, forensic reports, blockchain data, AI-generated attribution studies – that is often costly, technically sophisticated, and beyond the reach of the ordinary individual. Although such evidence was clearly dispositive in the SolarWinds (2020) and The DAO (2016) cases, [78] Additionally, there are no clear Palestinian laws or judicial standards to evaluate the reliability of scientific or technical evidence (similar to the U.S. "Daubert" standards), which would enable Palestinian judges to apply a reliable framework in admitting such evidence. [79]

Clause (a), on the other hand, specifically incorporates the classic common law limitation of "foreseeability" – i.e., damage is limited to that which was "foreseeable" or resulted "naturally" from the tort. In the world of advanced persistent threats and zero-day exploits (again, Solar Winds is the paradigm case), such a standard can easily lead to the exclusion of all damage on the theory that no reasonable person would have foreseen the particular attack vector used. In contrast, the "substantial factor" test used in many US jurisdictions greatly expands the range of recoverable damage. [80]

Taken together, these features of Article 60 – material-damage centrism, stringent particularity requirements, and foreseeability constraints – place Palestinian data-breach victims at a distinct disadvantage when measured against the more generous remedial landscape now prevailing in both the post-GDPR United Kingdom and large parts of the United States. [81]

4.2. Enhancing Integration Between Article 60 and Articles 50 and 55 bis.

Article 50 of the British Civil Wrongs Ordinance effective in the West Bank stipulates that civil liability requires proving that the act or omission was the direct or contributory cause of the damage, meaning it must be proven that the damage would not have occurred but for the act or omission, whether it was the sole cause or one of the contributing causes.

Article 50 focuses on the direct link between the act and the damage, making it an effective tool in simple cases, such as a company's negligence in protecting

[77] MyCrypto, 'Understanding Event Logs on the Ethereum Blockchain' (Medium, 4 March 2020).
[78] *Daubert v Merrell Dow Pharmaceuticals, Inc*, 509 US 579 (1993).
[79] Mandiant, *'Sunburst: A Sophisticated Supply Chain Attack*' (2020).
[80] Restatement (Second) of Torts § 431 (1965).
[81] OWASP, 'Zero Day Attacks' (2023).

customer data leading to a data leak. However, in complex cyber cases with multiple intertwined causes (like company negligence and hacker actions or victim negligence), applying the article may be difficult due to the lack of a clear framework for analysing intertwined causes.

Article 50 offers a robust approach to establishing causation, but there is a failure to address how intertwined causes, such as a hacker attack and negligence on the part of the plaintiff, will be managed. In fact, this could seriously weaken Article 50's potential impact on cyber-related cases, as evidence will inevitably involve a complex process of teasing apart a complex chain of technical circumstances and interlinked causes.

Take, for example, a hypothetical case where some contributory fault on the part of the customer himself/she herself, perhaps a weak password, clicking on a phishing link, or failing to enable two-factor authentication, played some contributory part. Article 50, standing on its own, offers little guidance on any means of quantifying that contributory fault, or how a potential adjustment might be made in consequence. Article 60 then adds an additional layer of requirements with regard to foreseeability and particularisation, making things even more difficult for the claimant.

What is really needed, however, to make Article 50 and Article 60 work coherently with one another in a cyber-related case is some form of interpretative guidance or a minor amendment to Article 50 that explains how contributory negligence is to be assessed, especially with regard to a harm suffered in cyberspaceFor instance, in the case of Surety, blockchain logs could provide evidence of causation; the lack of standards for analyzing intermingled causes within Article 50 can create complexity that impede the application of Article 60 if a third party, such as hackers, intervenes to contribute to the damage.

Integration with Article 55 *bis* (a, b, c):

The following article gives a more specific framework on how to establish causality and liability:

(a) " It ties liability to the breach of a statutory duty, and it requires that the damage be of the type which the legislation seeks to prevent. This is another way of expressing the principle of foreseeability, in that the damage must be a foreseeable consequence of the breach, and the clause is thus assimilated to the American concept of "proximate cause."

(b) " It does not include damage caused by unforeseen natural forces-events or deliberate negligence of another party, such as plaintiff's negligence or hacker intervention. This exemption narrows the frame within which one may be found liable in a case where the damage is caused by factors external to the system, sophisticated cyber-attacks being one variety of these. Zero-day attacks mean cyber-attacks conducted using unknown security vulnerabilities in software for which patches have not been released yet, or they are just unknown, so that those attacks cannot be predicted or prevented in advance. Correspondingly, the damages caused by them are legally excluded because of uncontrollable character".

c) "It permits a reduction of compensation according to the plaintiff's negligence, consistent with Article 60(b)'s criteria for itemizing damage; nevertheless, this will be perfected if the courts can develop legal tests on the

percentage of comparative negligence in cyber cases, for instance, whether the use of a weak password by a plaintiff is sufficient negligence to reduce compensation. In the The DAO case, it was partial investor negligence - failure to independently verify contract security - that contributed to the damage; thus, for compensation decisions under Article 60, the application could be made under Article 55 bis c)".

5. Conclusion.

The British Civil Wrongs Ordinance of 1944, amended by Law No. (5) of 1947, in force in Palestine, is a traditional legal system tailored in a historical setting utterly unlike the technical and legal intricacies imposed upon current cyber breaches. This can critically weaken the usefulness of the provision in cyber-related cases, because proof in those cases would almost always depend on untangling a complex series of technical events and overlapping causes.

For example, in the paradigm case of contributory fault or negligence on the part of the customer, such as the poor password, clicking on a phishing email, or failure to enable two-factor authentication, which contributed to the breach to some degree, there is nothing in Article 50 which appears to offer any guidance on measuring the degree of contributory fault and apportioning liability accordingly. Then, of course, there is the added layer of cake with regard to foreseeability and particularisation of loss under Article 60.

What would actually help to make these provisions work in harmony with one another in the digital world would be to provide interpretive guidance or a limited amendment to Article 50 to provide clarification on how contributory negligence is to be determined in cyberspace. The clarification that would be created by such an amendment would remove the confusion now existing and enable Article 60's procedural requirements to be sensibly and proportionally applied to data breach litigation.

1. The difficulty of proving causality in an environment where multiple players are involved-the service provider, the hacker, and the user-all connected in various way.
2. The insufficiency of provisions to keep pace with the type of moral damage arising from data violation, which cannot be measured in tangible ways despite its severity.
3. There are no standards on which to base "reasonableness" with regard to security measures required in the digital world; this provides much room for interpretation.

It follows then that this law must be developed with a proactive approach to legislation where development is based on:

- Assisting the systematic reform of existing legislations through the introduction of clear definitions of terms such as "personal information," "cyber breach," "duty of care in cyberspace," "cyber moral damages," etc., similar to the definitions provided in contemporary legislations such as the UK GDPR.
- Improvement of coordination between articles: Providing detailed judicial and interpretive directives that clarify the application of the

combination of articles (50, 55 bis, 60) of the existing legislation in cyber crime cases, especially during the analysis of the causation of damage in the event of concurrent negligence of the victim or the intervention of a third party.

- Reference to security standards: For example, the proposed National Data Protection Authority can create a guide that explains the meaning of "reasonable security measures" using international security standards such as ISO 27001 or NIST. This will ensure that there is an objective criterion that the judiciary can take into account while deciding whether an organization has fulfilled its duty of care or not.
- Development of judicial and technical capacities: Training judges and lawyers to understand the analysis of digital evidence and the creation of specialized judicial circuits.

Caggiano IA, 'Measuring contract transparency: from legal reasoning to LLM-based assessment. An italian law perspective' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252IAC

EJPLT
ISSN 2704-8012

Measuring contract transparency: from legal reasoning to LLM-based assessment. An italian law perspective

Misurare la trasparenza contrattuale: dal ragionamento giuridico all'impiego dei modelli linguistici. Una prospettiva di diritto italiano

ILARIA AMELIA CAGGIANO
Full professor of Private Law
Vice-director of the JM Centre of Excellence – ReCEPL4STAI
Università degli Studi Suor Orsola Benincasa

Abstract

Contract Transparency is widely recognised as a fundamental safeguard for individual self-determination. However, its inherent indeterminacy often undermines its practical effectiveness. This paper explores the possibility of translating qualitative transparency requirements into measurable and computable parameters in order to enhance the consistency, predictability, and legal certainty of the transparency assessments. Starting from a reconstruction of the legal meaning and function of transparency in contract law, with particular attention to Italian consumer and banking contract law, the article analyzes the logical-legal steps underlying the transparency assessment as a distinct interpretative operation for exploring both its measurability and its potential computational implementation. On this basis, the article discusses the extent to which the transparency assessment may be operationalized for LLM-based applications in support of judicial decision-making within the framework of human–AI collaboration.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
La trasparenza contrattuale è ampiamente riconosciuta come una tutela fondamentale per l'autodeterminazione individuale. Tuttavia, la sua intrinseca indeterminatezza ne mina spesso l'effettività. L'articolo esplora la possibilità di tradurre i requisiti qualitativi della trasparenza in parametri misurabili e computabili, al fine di accrescerne la coerenza, la prevedibilità e la certezza del diritto nelle valutazioni della trasparenza. A partire da una ricostruzione del significato giuridico e della funzione della trasparenza nel diritto dei contratti – con particolare attenzione alla normativa italiana in materia di contratti bancari e dei consumatori – l'articolo esamina i passaggi logico-giuridici alla base della valutazione della trasparenza come autonoma operazione interpretative, per esplorarne sia la misurabilità, sia la potenziale attuazione computazionale. Su queste basi, l'articolo discute la misura in cui il giudizio di trasparenza possa essere reso operativo per applicazioni basate su LLM a supporto della decisione giudiziale nell'ambito di una collaborazione uomo-IA.

Keywords: transparency; consumer credit contracts; contract transparency assessment; measurement; judicial decision; augmented justice

Summary: 1. Introduction. Dimensions of Transparency: Legal Norms and Language. – 2. Assessing Contract Transparency in Judicial Reasoning. – 3. Transparency in Action: Consumer Credit Agreements and the Judge Discretion. – 4. Conclusion. Measuring Contract Transparency: Computational Approaches and the Role of LLMs in Supporting Transparency Assessment.

1. Introduction. Dimensions of Transparency: Legal Norms and Language.

Transparency, as a legal norm, is widespread in contemporary law, taking on a variety of meanings. In the Italian legal system, it is required of public bodies and institutions in terms of openness and accessibility (right of access to documents);[1] in certain sectors, it specifies more general obligations related to the disclosure of information by entities towards clients, potential clients and markets[2].

Furthermore, transparency concerns acts and relations between individuals, such as in asymmetrical contracts, where a legal obligation to disclose certain information is provided for in terms of minimum content or formal requirements to achieve clarity, comprehensibility, and at times, conciseness.[3]

[1] In the Italian legal system, transparency in administrative law (Article 97 of the Italian Constitution) concerns the obligations of transparency regarding the public disclosure and dissemination of administrative acts, documents, information and data by public administrations (Legislative Decree No. 33 of 14 March 2013 and subsequent amendments), as well as the right of each individual to know precisely the content of the actions of public administrations (Law No. 241 of 7 August 1990 and subsequent amendments).

[2] An exemplary sector is banking, where the notion of transparency has broad application, referring both to information on the institution and its activities, and to features relating to the contractual relationship with the customer (*disclosure* obligations, institution governance rules and product control, supervisory powers of administrative authorities to protect the customer and the market, and customer information on banking services and operations). More recently, the impact of decision-making algorithms on banking has also emerged: see A Davola, *Algoritmi decisionali e trasparenza bancaria* (Utet 2020).

[3] The word "transparency" is expressly mentioned in some legislative texts (e.g., Articles 5(1)(a) and 12(1) of the GDPR) and in the recitals of EU legislation (*e.g.,* Directive 2008/48/EC), as well as in the Italian

Moreover, a legal obligation of transparency, regarding the content and means of information, is owed by data controllers when informing natural persons. [4] Lastly, it represents an ethical and legal requirement in developing technologies and Artificial Intelligence, encompassing the right to meaningful information and an *ex post* algorithmic explanation in the event of an AI decision not mediated by human evaluation (automated decision-making). [5]

In such a scenario, some scholars have argued that dealing with transparency in legal terms could be 'a scientifically unreliable and practically fruitless operation'. [6] Moreover, through the figurative use of the term 'transparency' in legal language, the notion has become homogeneously perceived in its axiological meaning, and for that reason, insidious. Like all legal metaphors, this figurative meaning bypasses the rational control. The comprehension of the concept is drawn to its meaning in general language and risks inducing the exchange of the figurative sense for (legal) reality.[7]

Therefore, if one refers to the meaning of an absence of any obscurity or intermediation in human cognition and, thus, to the values of certainty, truth, and rational knowledge and choice, transparency could be perceived in the legal domain as a safeguard and an instrument enabling fundamental values and rights, such as the protection of public interests, the competitive market, and the self-determination of the individual, regardless of any precise evaluations on its efficacy and effectiveness. [8] However, the concept of transparency is inherently indeterminate and its perception as a guarantee is misleading.

The content of what is regarded as "transparent information" remains uncertain. In private law, where information serves to enable self-determination, a mere standardized list of information, usually provided by law, might not even be read or understood by the relevant recipient, considering

---

Consolidated Banking Act (Testo Unico Bancario - TUB), Title VI. The word transparency appears again in the Italian Consumer Code both as a general normative value [Art. 2(2)(e)] and as a set of more specific requirements concerning clarity and comprehensibility (Art. 35), whose concrete content is shaped by judicial interpretation and legal scholarship.

[4] The distinction between an act and an activity, due to the different interests to be protected, entails different rules and controls, which have been explored in more depth in private law literature. See P Spada, *La tipicità delle società* (CEDAM 1974).

[5] On the relevant rules of the GDPR, a comprehensive review on the point is in E Troisi, 'Algorithmic Decision, Black-box and Ethical AI: The Right of Access as the Right to Obtain an Explanation' [2022] Jus Civ. 953 - 975. In the AI Act, transparency obligations are required at different levels: providers of high-risk AI systems (e.g., recruitment software, credit scoring) must provide deployers with instructions for use and technical interpretability (Art. 13) and natural persons have the right to an explanation of individual decisions made by deployers via high-risk systems (Art. 86); providers and deployers of limited-risk and generative AI systems (e.g., chatbots, image generators, deepfakes) must disclose AI interaction to end-users and apply watermarking to synthetic content (Art. 50); providers of general-purpose AI (GPAI) models must publish a summary of training data for copyright compliance (Art. 53).

[6] The quotation, referring only to the transparency of contracts, is from G Alpa, 'Note minime sulla trasparenza dei contratti bancari e finanziari' in P Ferro Luzzi and G Castaldi (eds), *La nuova legge bancaria. Il T.U. delle leggi sull'intermediazione bancaria e creditizia e le disposizioni di attuazione. Commentario,* III (Giuffrè 1996), 1783, already taken up by S Pagliantini, 'Trasparenza contrattuale', *Enciclopedia del diritto Annali V* (2012) 1280 ff.

[7] See F Galgano, *Le insidie del linguaggio giuridico. Saggio sulle metafore del diritto* (Il Mulino 2010).

[8] For a radical critique of the society of transparency (as an instrument of surveillance), see B-C Han, *La società della trasparenza,* trans. F Buongiorno (Nottetempo 2014), who interprets transparency as a false ideal.

the well-known limitations of rationality, cognitive biases, heuristics, and the risks of cognitive overload for the information recipient.[9]

In the more specific realm of data protection, for instance, where there is a requirement for the controller to inform 'in a concise, transparent, intelligible, and easily accessible manner, in simple and clear language,' even a compliant privacy notice may not be able to directly guide the decision, *i.e.,* informational self-determination due to the complexity of the domain itself to be understood. Instead, it primarily serves as an instrument for *ex post* control.[10]

In the context of asymmetrical bargaining, rules of informational transparency intended to address information asymmetry may not only fail to solve the contractual imbalance, but risk merely shifting responsibility onto the recipient of the information (the weaker party), who, having been informed, is deemed to have effectively chosen.[11] They are also ineffective if they are viewed solely as affecting the professional's conduct in the pre-negotiation phase, since they would be protected exclusively through the remedy of damage compensation and would load the claimant with a heavy burden of proof.

However, one must consider that within asymmetrical negotiations, transparency assures a certain degree of protection to the weaker party to the contract,[12] as demonstrated by the increase in judicial and extrajudicial litigation on the transparency of contracts.[13] Nevertheless, the emerging litigation and the sanctions of professionals' opportunistic behavior still reveal a lack of defined indexes of transparency.

This article aims to investigate this question, namely the conditions under which a contract may be considered transparent, by analysing the stages of the

[9] L Gatt, R Montanari and IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico – comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' [2017] Politica del diritto, 39 ff.

[10] See IA Caggiano, 'Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali' [2018] ODCC, 67-104, esp. 89.

[11] See A Barenghi, 'Appunti sulla trasparenza bancaria, venticinque anni dopo' [2017] Questione Giustizia (online journal).

[12] The protection of the weaker party through transparency can be understood in multiple ways. First, transparency operates as a criterion for choosing among possible interpretations of the contractual text (rather than as a remedy in the strict sense): in cases of doubt, ambiguous terms must be interpreted in the way most favourable to the consumer, pursuant to Article 35 of the Consumer Code and Article 1375 of the Civil Code. Secondly, transparency also plays a role in the assessment of unfair terms. Where contractual terms concern the subject matter of the contract or the adequacy of the price, the sanction of nullity provided for by Article 34(2) of the Italian Consumer Code may apply if such terms have not been drafted in clear and intelligible language. This sanction therefore represents a further stage in the assessment of unfairness. Thirdly, where contractual terms are not comprehensible to a person of average ability and intelligence, they cannot produce effects against the consumer, who is nevertheless required to exercise ordinary diligence in becoming aware of their content (by analogy with Article 1341 of the Civil Code). Finally, an absolutely incomprehensible clause is void for lack of determinacy of the object. On this point, CM Bianca, 'Il Contratto', *Diritto civile III* (Giuffrè 2019) 356 ff.

[13] One thinks, for example, once again of the banking sector and the operation of out-of-court dispute resolution bodies such as the Banking and Financial Arbitrator (ABF), which have made it possible for previously hidden litigation to emerge due to the modest value of the dispute, in which the issue of transparency (of contractual terms and conditions) is central. See the report on the activities of the ABF in 2022 (data for 2021 and the first months of 2022). In general on this subject, A Barenghi, *Consumer Law* (2nd edn, Wolters Kluwer 2020) 466 ff.

interpretative assessment (hermeneutical judgement) of transparency and the application of logical and linguistic criteria in contract interpretation.[14-15]

Secondly, it explores the potential role of technologies and methodologies, such as Artificial Intelligence and LLMs, in this interpretative process from the perspective of the judicial decision-making. Far from implying the complete automation of judicial reasoning, this perspective encourages a reconsideration of the human cognitive processes underlying judicial assessments.[16]

To develop this twofold objective, the paper is structured in three main sections. After reconstructing the legal framework of contract transparency under Italian law, the analysis turns to its judicial assessment in practice, with particular attention to consumer credit agreements as a field where the evaluation of comprehensibility and the protection of vulnerable parties have become particularly significant. The final part explores the possibility of translating transparency requirements into measurable parameters, investigating how technological tools and artificial intelligence may contribute to a computational assessment of contract transparency while preserving the normative and contextual dimension of judicial reasoning.

2. Assessing Contract Transparency in Judicial Reasoning.

When assessing the transparency of a contractual text, especially in the context of an asymmetrical business-to-consumer contract, the interpreter (*e.g.*, a judge, but also a party to the contract) must evaluate the *quality of the text* in terms of clarity, comprehensibility and accessibility to the weaker party. This involves determining whether the text has been written clearly and comprehensibly (as outlined in Article 35 (1) of the Italian Consumer Code, which refers to the *clarity and comprehensibility* of the contractual text),[17] according to the social sphere where statements are made, *i.e.* for the group of customers for whom the contract is intended (the average consumer).[18] In credit contracts, it must also be assessed also whether specific relevant information has been provided in a concise manner (*e.g.,* as specified in Article 125 *bis* of the Italian Banking Act - TUB).[19] In banking contracts, some specific

[14] J Nieva-Fenoll, *Intelligenza artificiale e processo* (Giappichelli 2018) and A Guarapon and J Lassègue, *La giustizia digitale* (Il Mulino 2021).

[15] This aspect specifies the characterisation of law as a cultural subsystem, which manifests itself through language (and social practice), on this point, commenting on Falzea's thought, P Sirena, 'Teoria dell'efficacia giuridica nel pensiero di Angelo Falzea' [2017] Riv. dir. civ., 999 ff.

[16] M Frixione, *Come ragioniamo* (Editori Laterza 2021), which enucleates decision-making among the cognitive processes, in addition to inferences and *problem solving*, all of which converge in the judge's interpretative and decision-making process.

[17] S Martuccelli, 'Il canone dell'interpretazione più favorevole al consumatore' in Aa. Vv., *Studi in onore di Giuseppe Benedetti* (2008) 1015 ff., esp. 1024.

[18] With regard to boilerplate clauses, addressed to an indistinct class of contracting parties, the yardstick for assessing comprehensibility is the average consumer*, i.e.*, an abstract and general parameter not referring to particular semantic capacities, see Martuccelli (n 17) 1025 ff. Even in the case of banking contracts, for which the transparency regulations (Bank of Italy Transparency Provisions, para. 12 *General Principles*) lay down differentiated modalities in relation to the different customer groups and the characteristics of the services, personalised contractual information has not been achieved. On this subject, in a critical sense, AA Dolmetta, *Trasparenza dei prodotti bancari. Rules* (Zanichelli 2014) 88 ff.

[19] On the safeguards protecting this notion of transparency, see *supra* n 12.

canons of clarity and comprehensibility are provided, though limited to the stage prior to the conclusion of the contract (e.g. graphic highlighting using a representative example, Art. 123 TUB).

The transparency assessment is a hermeneutic process which constitutes a distinct evaluative step within the legal interpretation of the contract. While legal interpretation *stricto sensu* aims to identify the legal meaning and ascertain the substantive content of the parties' rights and obligations - also considering the parties' bahaviour following the signing of the contract - the transparency assessment is focused only on the contractual text on the way in which contractual terms are formulated and presented (art. 35 Cons. Code), in light of protecting the weaker party. A finding of non-transparency may, moreover, trigger specific legal remedies provided by law and distinct from those provided for by the rules of interpretation: interpretation in favour of the consumer as *per* Art. 35 (1) of the Italian Consumer Code, or nullity under Art. 34 of the same Act when the ambiguity refers to the object of the contract and adequacy of the consideration.[20]

However, these two processes remain closely interconnected, as they both refer to the meaning of the contract in order to ascertain its content or qualify it.

Transparency of contractual content implies that relevant information is presented to ensure completeness and an adequate understanding of the consequences arising from the agreement (*comprehension*). Moreover, the evaluation of transparency requires considering the legal canons set out in Italian law in Articles 1362–1366 of the Civil Code on contractual interpretation, which also provide a framework for assessing transparency, where compatible,[21] as far as they are applicable to consumers as well.

According to the prevailing view among legal scholars, contract interpretation constitutes a factual judgment,[22] namely an assessment on the merits rather than a review of legality. It involves the application of legal rules,

[20] On the relation between Art. 35 (1) and 35 (2) of the Italian Consumer Code and Art. 1370 of the Civil Code, see Martuccelli (n 17) 1050 ff.

[21] Under Italian law, the contract interpretation criteria are deemed to be structured into three distinct groups, hierarchically structured, from Articles 1362 to 1371 of the Italian Civil Code. The first group comprises criteria for subjective interpretation (the common intent of the parties): Article 1362 (Intenzione dei contraenti), Article 1363 (Interpretazione complessiva delle clausole), Article 1364 (Espressioni generali), and Article 1365 (Indicazioni esemplificative). Article 1366 (Interpretazione di buona fede) dictates that all contracts must be interpreted in accordance with the principle of good faith. Criteria for objective interpretation are aimed at resolving ambiguity via Article 1367 (Conservazione del contratto), Article 1368 (Pratiche generali di interpretazione), Article 1369 (Espressioni con più sensi), Article 1370 (Interpretazione contro l'autore della clausola), and Article 1371 (Regole finali). As for the hierarchical structure of these interpretative criteria, in line with the theory of Grassetti see N. Irti, *Testo e contest* (Padova 1996). Whatever position is taken regarding the relationship between the subjective and objective criteria of interpretation, this article argues that the first set of criteria, together with the principle of interpretation in accordance with good faith, should also be taken into account for the purposes of assessing contractual transparency. They form part of the interpretative framework that the consumer or other weaker contracting party is expected to employ in understanding the contractual text. By contrast, recourse to the objective criteria of interpretation presupposes ambiguity or opacity of the contract. From the perspective advanced in this article, they apply only when the meaning of the contractual term remains unclear through the ordinary interpretative tools available to the average addressee. This conclusion is consistent with the wording of the relevant provisions, which make the objective criteria applicable only where there is uncertainty or ambiguity in the understanding of the contract (*i.e.*, lack of transparency). Such uncertainty presupposes already a finding of non - transparency.

[22] See, albeit critically, V Calderai, *Interpretazione del contratto e argomentazione giuridica* (Giappichelli 2008).

linguistic criteria, technical knowledge and rules of experience, as also recognised within the legal framewrok.[23] This is true also for the assessment of transparency.

From this perspective, the transparency assessment may be viewed as a syllogistic judgment embedded in the polysyllogistic structure of contract interpretation.[24] Indeed, linguistic rules, rules of experience, and hermeneutic canons provided by law constitute major premises of instrumental inferences, as they fix the case in a preparatory function for the final step of ascribing the fact to the norm.[25]

The first level of the syllogism implies knowledge and application of linguistic rules and semantic codes. Regarding the relationship between the professional and the average consumer, they include primary codes, *i.e.*, the linguistic usages current in the entire linguistic community at a given time, and possible sub-codes.

It has been emphasized that literal meaning, as a methodological canon, is inherently a guarantee of meaning: it implies a finite number of meanings, and language, as a formal system of meaning, constitutes an insurmountable domain, the logical limit of meaning and the condition of its predictability and verifiability.[26] However, in the transparency assessment to verify clarity and comprehensibility, as it is in the interpretive judgment for the choice between meanings, it involves the construction of a network of meanings within the entire contractual text, syntactic constructs, and an internal logic. It requires identifying the cognitive horizon of the average consumer in order to assess whether the contractual terms are *comprehensible*, ambiguous, or unclear, and whether they enable the consumer to understand the legal *consequences* of the contract.

In this regard, it could be said that the interpreter operates using his/her own ability to understand within this complex network the common meaning and the interpretation(s) closest to the average consumer[27] under given external conditions.

Yet, neither from the point of view of language nor from that of expression, are there rules of linguistic clarity that professionals are obliged to follow when contracting with the consumer. Indeed, one must also consider that in some sector regulations (in particular, in the instructions of the Authorities, such as the banking sector) one can find drafting indications, which constitute linguistic, typographic, lexical, and syntactical guidelines, relevant at the industry level, and capable of affecting the conformation of contracts. [28]

---

[23] C Grassetti, *L'interpretazione del negozio giuridico* (CEDAM 1983) speaks more properly of a logical-legal procedure, not of a pure factual judgement.

[24] Calderai (n 22) 93.

[25] Calderai (n 22) 435.

[26] M Orlandi, *Introduzione alla logica giuridica* (Mulino 2021), 95, where a «sistema formale di senso […] costituisce un dominio invalicabile, limite logico del significato e condizione di prevedibilità e verificabilità dello stesso».

[27] On the bounded rationality of consumers, a factor increasingly taken into account in judicial reasoning: see Council of State 10/10/22 no. 8650, in *Onelegale* database. In the literature, A Zoppini, 'Contratto ed economia comportamentale', *Enc. giur. tematici* I *Contratto* (2021) 313 ff. On biases in legal reasoning, L Calcagno, G Grassi, G Positano (eds.), *Psicologia del giudicare, Quaderno 32 SSM* (2024) 124 ff.

[28] See Transparency provisions applying to banking operators, Bank of Italy, *Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e client*, 19 March 2019. *In* particular, Annex 1 of the Provisions provides a guide with the main drafting guidelines that intermediaries can apply

Moreover, there are uniform standards that aim to provide criteria for clear writing translated into shared recommendations, such as the necessity of planning the text before writing, choosing familiar and concrete words, constructing syntactically linear sentences, and adopting precise strategies for the visual organization of information.[29] However, none of them is focused on contractual language. Both the guidelines and the standards traces back to the plain language technical approach, which is rooted in psycholinguistic studies and considers three levels (wording, structure, and design) to define the clarity of information.[30]

While not binding on the interpreter, these guidelines can help ascertain the perspective of the search for transparency, along with the relevant studies on professional and specialized language.[31]

3. Transparency in Action: Consumer Credit Agreements and the Judge Discretion.

Banking contracts contain terms and conditions (boilerplate clauses) regarding applied costs, synthetic cost indices, rules of the contract, and reimbursement mechanisms limited to only some of the costs and commissions, such as in the case of early repayment. To make an informed choice, consumers should understand both the economic content as well as the contractual legal rules. The judge (or interpreter), through an *ex post* prognostic assessment, must determine whether the consumer, based on the average consumer parameter, has been placed in a condition to understand the contract terms.

If we look at some of the controversial cases that have attracted attention at the national and European levels, we can highlight how the opacity of clauses is assessed on the basis of specific criteria. These criteria consider the complexity of the economic transaction as a whole (and consequently, the complexity of the notions to be understood), the connections between meanings within the entire contractual text (and thus, the connections between different clauses), and a common sense test.

---

in their disclosures, such as, e.g.: the use of different font styles to highlight information; the use of bulleted lists and tables; the structure of documents to facilitate comparison; and verb forms and the most comprehensible pronominal usage.

[29] The relevant standards are UNI ISO 24495-1:2024 and the more recent ISO 24495-2:2025. While UNI ISO 24495-1:2024 is a general and universal document, intended for standard printed or digital texts aimed at a broad audience, ISO 24495-2:2025 specifically addresses the ecosystem of legal communication. According to the latter, legal documents must tackle a dual challenge: maintaining the utmost technical accuracy required by law while simultaneously being understood by citizens or managers who lack specific legal training. To achieve this, the second part introduces tools, such as collaborative writing processes from the very first drafts involving legal professionals and experts in legal design.

[30] On the Plain language movement, JC Redish, 'The Plain English Movement', in S Greenbaum (ed.), *The English Language Today* (Pergamon Press 1985) 125-138; D Fortis, 'Il plain language quando le istituzioni si fanno capire' *I Quaderni del MdS* (2003) available at <https://www.mestierediscrivere.com>. In Italy, rules of plain language were proposed for public administration see Presidenza del Consiglio dei Ministri – Dipartimento della funzione pubblica, *Codice di stile delle comunicazioni scritte pubbliche ad uso delle amministrazioni pubbliche* (Roma 1994).

[31] G Acerboni, A Panunzi, 'La scrittura professionale' in B. Baldi (ed.), *Comunicare ad arte*, Bologna (Zanichelli 2020) 221 ff., where the authors argue for the necessity that specialized writing comply with rules such as the standard UNI ISO 24495-1.

If one takes as an example the case of real estate loans indexed in foreign currencies, as emerged in ECJ and national case law, he/she will find compounding mechanisms for calculating the interest due. In a number of disputed domestic cases, the contract also contained a translation error related to early repayment.[32] In any case, the contract allowed the borrower to repay the mortgage early, stating that the principal to be repaid and any arrears were first calculated in Swiss Francs (CHF) using the contractually fixed exchange rate, and then converted back into Euros (EUR) based on the current market exchange rate on the day of repayment.

Authorities (judicial, administrative, and extrajudicial) have deemed the clause obscure, empolying a reasoning that can be traced back to the divergence between the common sense of the transaction and the text, even formally and grammatically intelligible, in the context of a complex transaction. To this extent, the Courts have repeatedly stated that financial institution must provide the borrower with sufficient information, including, where appropriate, simulations or concrete calculation examples of the risk, or that information relating to the past performance of the index on the basis of which the calculation is made, as well as simulations illustrating scenarios of fluctuation and the corresponding financial impact. [33]

On the other hand, in litigation concerning the reduction of costs incurred in connection with credit agreements due to early termination, which has recently drawn the attention of the Constitutional Court, [34] a focus on contractual transparency emerged. The question, as far as it concerned transparency, related to the content of specific clauses describing pre-contractual activities and, in particular, whether in each of these terms the words used exactly and clearly referred to activities prior to the conclusion of the contract, or if they were unclear and implied also activities subsequent to the conclusion of the contract (as is evident in expressions such as "management activities", "postage", "documentation"). In the second case, where words used were not homogeneous with the rest of the clause's text, its heading, and its regulation, the clause was considered opaque, leading to the application of the more favorable rules (those relating to executive activities), i.e. the mandatory rules.

[32] An exhaustive reconstruction of the cases is in Dolmetta and Lentini (n 18) 1 ff.

[33] See, Case C-125/18 (§51) *Marc Gómez del Moral Guasch* v *Bankia SA* EU:C:2019:695, available at <https://curia.europa.eu> followed by the national case law, cited below. See also, Case C-26/13 *Árpád Kásler, Hajnalka Káslerné Rábai* v *OTP Jelzálogbank Zrt* EU:C:2014:282; Case C-51/17 *OTP Bank Nyrt., OTP Faktoring Követeléskezelő Zrt.* v *Teréz Ilyés, Emil Kiss* EU:C:2018:750; Case C-448/17 *Árpád Kásler, Hajnalka Káslerné Rábai* v *OTP Jelzálogbank Zrt* EU:C:2014:282; Cass. civ, Sec. I, Judgment, 31/08/2021, no. 23655 in Onelegale database; Arbitro Bancario Finanziario, Collegio di Coordinamento, decision no. 5866/2015; AGCM, decision no. 27214/2018, in Bulletin no. 26 of 9 July 2018; *contra* Tribunale di Roma, judgment 21 January 2019, in <www.expartecreditoris.it>. Following the precedents of the Court of Justice of the European Union, the Courts have stated that contractual transparency in foreign currency mortgages must go beyond mere grammatical clarity to ensure that the average consumer can fully comprehend the concrete economic mechanism and evaluate the financial consequences of exchange rate risks on their total debt. Consequently, financial institutions are legally required to provide comprehensive pre-contractual information so that borrowers can make prudent, well-informed decisions. Ultimately, any obscure clauses regarding the main subject matter, such as currency conversion, that create a significant imbalance to the consumer's detriment can be deemed unfair and declared completely null and void.

[34] Constitutional Court, Judgement No. 263 of 22/12/2022, in www.cortecostituzionale.it.

The extensive litigation concerning these cases revealed the opportunistic behavior of professionals in unclearly classifying the relevant clauses.[35]

As anticipated, the current analysis focuses on the transparency assessment of term wording and its meanings.

4. Conclusion. Measuring Contract Transparency: Computational Approaches and the Role of LLMs in Supporting Transparency Assessment.

Once the concept of transparency has been specified, a further question may arise: whether transparency can be measured, *i.e.*, assessed through quantitative parameters. The issue is not merely a methodological one. Translating the factors and criteria that underlie assessments of transparency into quantitative indexes may help provide a more structured framework for judicial evaluation, thereby enhancing the consistency and predictability of judicial decisions and deflating litigation.

Moreover, translating the transparency assessment into measurable parameters opens up a broader inquiry into the computability of transparency. To the extent that the relevant elements of the judgment can be formalised, technological tools – including Artificial Intelligence – may contribute to supporting, modelling, or partially reproducing some aspects of the transparency assessment.

Considering the logical steps of the transparency assessment, the development of studies on plain language, and the examples taken from European and national judgments, measurable parameters of transparency may be evaluated, starting from legal canons which lay down literal and contextual interpretation, as well as common rules for general expressions and examples. These parameters for measuring can be derived from different levels:

- textual linguistics, which provides criteria for analyzing a text as a whole, in terms of its communicative function and acceptability for the addressee, its internal coherence, cohesion, and architecture of information (*e.g.*, through the theme – rheme progression) taking into account the context in which it is produced;
- specialized language lexicon and morphosyntax[36]

[35] Constitutional Court, Judgement No. 263/22: '*Faced with the distinction between up-front costs, which are non-recoverable, and recurring costs, which can be reduced, in reality abusive conduct emerged in the qualification and allocation of costs; the ABF reacted to this - in its decisions - by providing that, in the face of non-transparent conduct, all costs whose reasons had been opaquely manifested should be deemed reimbursable when the contractual conditions were drawn up*' (translation is ours).

[36] Acerboni and Panunzi (n 31) 233 ss. In the medical domain, for a complete framework for medical language as specialistized language, L Moro, 'Accessibilità e semplificazione linguistica nei testi di ambito medico ad uso del paziente: un esempio di buona pratica' (thesis, Università Ca' Foscari, 2018) 27 ff.; S Rinnone, 'Analisi della leggibilità dei consensi informati: un approccio linguistico-computazionale' (thesis, Università di Pisa, 2016) 1- 124.

- the plain language approach, which has developed indexes in general and specific sectors in continuity with textual linguistics[37] and has been developed, although on a general level, in standards,

- the applied psycholinguistics level;

- the presence of examples, to clarify the content and subject matter of the contract (*e.g.*, its economic value and consequences); the coherence between the meaning of individual words and the context of the clauses or terms where they are inserted;

All these rules should be considered in the assessment process in light of enabling the consumer to make an informed decision and considering inferential and predictive models.

By mapping the relevant elements in the transparency assessment, it becomes possible to model the algorithmisation of certain activities, aiming at increasing the certainty and celerity of the judgement as well as reducing litigation. Algorithmising the transparency assessment does not imply the complete reproduction of judicial reasoning within an artificial environment. Rather, it requires the identification and formalisation of the relevant parameters underlying the transparency assessment, to make them computable and measurable. The outcomes produced by computational models, including LLM-based systems, must then be empirically evaluated in light of legal standards and judicial reasoning.

As we have seen, the interpretative activity on contractual transparency may entail the identification of 'idiosyncratic' meanings within lists of words in terms regulating specific types of activity (to be concluded before the signing of the contract), or a more complex work of interpretation that relates to the understanding of the text, taking into account the description of a complex activity, the connections between the various phases of the contractual relationship, and the identification of the unclear meaning in this context.

At present, the prospect of the computability of the transparency judgement still appears to be in a development phase but can be approached in light of currently existing technologies.

The measuring task can be conducted in different ways: using purely quantitative software capable of verifying the degree of readability of a text according to different social and cultural groups (readability indices); encompassing in the first one comprehensibility indices;[38] or constructing AI

[37] E Cornelius 'Defining 'plain language' in contemporary South Africa' (2015) 44 Stellenbosch Papers in Linguistics, 1 ff., at 3.

[38] For the analysis of readability, the following can be considered: the Flesch index or, for the Italian language, the *Gulpease* index, and the core vocabulary (which for the Italian language is the Italian Basic Vocabulary (Vocabolario di Base) developed by Tullio De Mauro, Il Nuovo vocabolario di base della lingua italiana available at <https://www.internazionale.it/opinione/tullio-de-mauro/2016/12/23/il-nuovo-vocabolario-di-base-della-lingua-italiana>. From a linguistic point of view, comprehensibility can be analysed through text analysis from a linguistic and conceptual point of view. See E Piemontese, La scrittura: un caso di "problem-solving", in AR Guerriero (ed.), *Laboratorio di scrittura. Quaderni GISCEL* (La Nuova Italia 2002) 3-40, at 26. An attempt at encompassing lexical, morphosyntactic and syntactic parameters is currently, for the Italian language, in the tool READ-IT, available at <https://www.ilc.cnr.it/dylanlab/apps/texttools/?tt_user=guest>. A good description of the computational linguistic tool for legal language is in G Venturi, *Lingua e diritto: una prospettiva linguistico-computazionale*, (doctoral thesis, Università degli Studi di Torino, 2008-2011).

systems capable of assessing the clarity/readability and comprehensibility including additional and specialized parameters of transparency. [39-40]

The first two kinds of assessments relate to the industry-wide attention to the editorial criteria of texts (although not strictly contractual), which partly coincides with, and partly could augment, the currently usable readability and comprehensibility indices. These indices in their most sophisticated formulation calculate not only sentence and word length ratios, but also lexicon, syntax, the number of verbs (and nominalisations) and/or complements, and verbal forms, enabling an evaluation based on a standard user level. Such software neither recognizes nor is instructed with criteria proper to legal language and syntax.[41] For this reason, although they fail to intercept the characteristics and needs proper to legal language, they may be suitable for measuring, probably by default, the level of readability of a contractual text and may only constitute an initial measuring instrument.

Research in this area draws on computational linguistics and Natural Language Processing (NLP) techniques applied to legal texts. These approaches enable the calculation of quantitative linguistic and semantic indicators, such as lexical density, tokenization measures, syntactic complexity, and other text-based metrics, with the aim of assessing and modelling the comprehensibility and transparency of contractual language.[42]

Far from encompassing all components of transparency, these automatic and computational tools are not yet widely in use in the legal domanin.

Moreover, operationalizing the conditions for reading a text does not necessarily entitle one to understand it. The identification of unclear areas of texts, in light not only of the occurrence of certain linguistic forms, but based on texts that have already been recognized as obscure in jurisprudential experience or by empirical studies, could represent a support (and an *alert*) for the interpreter and a safeguard for the recipient of information.

The landscape could change with the advent of generative AI and the increasing capabilities of Large Language Models (LLMs). While research on contracts conducted using expert systems has shown that the main challenges lie in the construction of extensive databases, the costs and time required for initial training, and the mitigation of bias,[43] the emergence of Large Language Models (LLMs) may create new opportunities in this field. However, the use of LLMs to assess contractual clarity and transparency has not yet been the

[39] F Ruggeri and others, 'Detecting and explaining unfairness in consumer contracts through memory networks' (2022) 30 Artificial Intelligence and Law, 59-92; N Kolt, 'Predicting Consumer Contracts' (2022) 37 Berkeley Tech. L. J., 71 – 138.

[40] A first account is in B Boi and others, 'On exploiting LLMs and statistical methods for testing contractual clarity in legal contracts' (2025) *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing, SAC '25*, New York, 1299–1300.

[41] One example is the Dylan software, developed by the CNR.

[42] A Bajceta and others, 'Using NLP tools to detect ambiguities in system requirements - A comparison study' (2022) *NLP4RE 2022: 5th Workshop on Natural Language Processing for Requirements Engineering*; Soavi, Mylopoulos, and M Soavi and others, 'Contratto – A Method for Transforming Contracts into Formal Specifications' in R Guizzardi, J Ralyté, X Franch (eds) *Research Challenges in Information Science. RCIS 2022. Lecture Notes in Business Information Processing* (Springer 2022) vol 446; K Upadhyay and others, 'Is Your Legal Contract Ambiguous? Convert to a Smart Legal Contract' (2020) *IEEE International Conference on Blockchain* (Blockchain), Rhodes, Greece, 2020, 412-418.

[43] On privacy policies G Grundler and others, 'Detecting Vague Clauses in Italian Privacy Policies Using Transformers, LLMs, and Cross-Lingual Techniques' in ECAI (2025) 459 ff.

subject of systematic investigation. Empirical research investigating whether LLMs can reliably measure and predict the transparency of contractual terms remains scarce.[44]

Most studies conducted so far have focused on broader interpretative tasks. A growing body of research has explored whether LLMs can identify the meaning – or possible meanings – of legislative and contractual provisions [45], thereby evaluating their ability to interpret legal texts. Other studies have examined whether LLMs can recognize and apply legal interpretative canons and hermeneutic principles.[46]

The assessment of legal text quality and the measurement of transparency constitute a distinct legal task. While it necessarily presupposes some degree of textual interpretation, it is not exhausted by it. It requires the evaluation of linguistic, semantic, and structural features that affect the comprehensibility of legal documents for their intended audience.

In particular, LLMs' ability to capture inferences, implicit meanings, and pragmatic aspects of language, may pave the way for the development of tools for legal text analysis, [47] with the final aim of avoiding empty formalisms and self-serving measurements.

These capabilities could be explored by including the transparency assessment parameters to realize the following objectives:

1)Extend first-generation readability metrics and comprehensibility indices[48], to comprehensive criteria of plain language and specialized language.

2) Evaluate the semantics of individual clauses, as well as that of the entire document to appraise the overall informational architecture and cohesion offered to the consumer, accounting for cross-references.

3) Assess informational *completeness* as intended above by evaluating whether the contractual text makes the relevant consequences and effects of the agreement (economic and legal) sufficiently explicit, rather than hidden or left to complex inferences, *e.g.*, through examples and the strategic placement. This objective requires the comparison between the LLM's assessment and human tests on the same tasks.

These computational needs can be addressed through a methodological architecture available for LLMs:[49]

---

[44] Boi and others (n 40).

[45] C Engel and RH McAdams, *Asking GPT for the Ordinary Meaning of Statutory Terms, Public Law and Legal Theory Research Paper n. 848* (University of Chicago Law School 2024) 1–43; V Janecek and G Sartor, *Legal interpretation and AI: from expert systems to argumentation and LLMs, Forthcoming in International Handbook of Legal Language and Communication: From Text to Semiotics* (Springer 2026).

[46] E Martínez, 'Traditional and Computational Canons' (forthcoming 2026) 39 Harvard Journal of Law & Technology. Available at SSRN: <https://ssrn.com/abstract=5155444> or <http://dx.doi.org/10.2139/ssrn.5155444>.

[47] On LLMs' growing competence in pragmatic language understanding, see S Eo and H Lim, 'Unveiling the Limits of Large Language Models in Inferring Pragmatic Meaning from Non-Verbal Responses' (2026) arXiv:2606.01845v1 [cs.CL]; A Hota and JPP Jokinen 'Implicature in Interaction: Understanding Implicature Improves Alignment in Human–LLM Interaction' (2025) arXiv:2510.25426v1 [cs.CL].
It must be taken into account that while specific experiments on Unfair Clause Detection show that BERT-based models can yield better results than LLMs for clause classification tasks, a true judicial assessment of transparency inherently requires evaluating the global discursive structure.

[48] See above text correspondig to notes 38–40.

[49] Recent research on this point and the combination of these methods is being conducted by the Legal Clarity group at the ReCEPL Research Centre of Private Law (Suor Orsola Benincasa University of Napoli), especially within the project BACT&AI See the website <https://www.legalclarity.eu/bactai/>

1) Retrieval-Augmented Generation (RAG) Integration, to connect the LLM to a controlled dataset specifically trained on obscure and transparent clauses to ground the dataset definition;

2) Prompting Strategies, to prompt the LLM with a set of formal transparency rules (specific clarity elements described in psycholinguistic literature, pragmatic intelligibility criteria established by the Court of Justice of the European Union (CJEU) jurisprudence, and Plain Language rules) and to condition the LLM to simulate the cognitive and cultural competencies of the contract's specific recipient (the average consumer).[50]

The experiments made as well as a broader ethical view of the development of technology need to be taken into account in a project that aims to enhance the transparency assessment from a perspective of certainty and calculability.

The comprehensibility of a contractual legal communication entails compliance with general linguistic rules, but is also related to the specialized language, and sub-languages thereof, which in turn are characterized by specific terms, syntactic constructs, argumentative configurations, as well as the structure of the experience of the author and the (non-expert) recipient of the same.[51]

In this scenario, LLM capabilities should be driven by the intersection of computer science and legal expertise, aiming to identify optimal levels of human-machine collaboration through reliable testing and system designs engineered to prevent automation bias or undue influence on users.

[50] However, on the unexpected result of the "persona prompting" see EA Posner and S Saran, *Silicon Formalism: Rules, Standards, and Judge AI* (University of Chicago Law School Coase-Sandor Institute for Law & Economics 2026) Research Paper No. 26-02, where it was found that the LLM adheres to the legally correct outcome significantly more often than human judges.

[51] MA Cortellazzo, 'Giuridico-amministrativo, linguaggio', *Enciclopedia dell'italiano online* (Treccani 2010).

Capellà i Ricart A, Roig Batalla A, 'The Expanding Notion of Special Categories of Data and its Limits' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252ACRARB

EJPLT
ISSN 2704-8012



The expanding notion of special categories of data and its limits

L'espansione della nozione di categorie speciali di dati e i loro limiti

ANNA CAPELLÀ I RICART
Postdoctoral Researcher
Universitat Autònoma de Barcelona

ANTONI ROIG BATALLA
Full professor of Constitutional Law
Universitat Autònoma de Barcelona

Abstract

Building on Solove's warnings on the uselessness of the notion of special categories of data, this article examines the expansion of the concept in the CJEU jurisprudence to assess if, indeed, it has become futile in the EU context. Our research explores how the concept has been expanded to inference, its specific application in the context of the right to be forgotten, and its role in social networks and competition law. We highlight that the current understanding of data of special categories presents limitations in terms of providing an effective protection in the field of big data analytics and we theorise on the suitability of shifting from an exhaustive list of data categories to a more general risk-based approach.

Muovendo dalle riflessioni critiche di Daniel J. Solove in merito alla scarsa utilità della nozione di categorie particolari di dati, il presente contributo esamina l'evoluzione ed espansione di tale concetto nella giurisprudenza della Corte di giustizia dell'Unione europea, al fine di verificare se esso sia divenuto, nel contesto dell'Unione europea, sostanzialmente privo di rilevanza operativa. L'analisi si concentra, in particolare, sull'estensione del concetto alle inferenze, sulla sua applicazione nel contesto del diritto all'oblio, nonché sul ruolo che esso assume nell'ambito dei social network e del diritto della concorrenza. Si evidenzia come l'attuale configurazione delle categorie particolari di dati presenti significative criticità sotto il profilo dell'effettività della tutela nell'era delle analisi di big data; in tale prospettiva, si propone una riflessione circa l'opportunità di superare un approccio fondato su un elenco tassativo di categorie, a favore di un modello più flessibile e generale, incentrato sulla valutazione del rischio.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: data of special categories; GDPR; inference; big data; expansion

Summary: 1. Introduction. – 2. The limited and selective expansion of the notion of data of special categories in the CJEU jurisprudence. – 2.1. The limited acceptance of inference in CJEU jurisprudence. – 2.2. The right to be forgotten: a latent generalisable expansion of special categories of data via the balancing test of Article 9(2)g) GDPR, and upon request. – 2.3. A potential game-changer: protecting data of special categories on social networks through competition law. – 3. The limits of the notion of data of special categories. – 3.1. Inferences of data of special categories in big data analytics. – 3.2. Special-category data, legitimate interest and AI model training. – 4. Conclusions.

1. Introduction.

Solove held recently that the General Data Protection Regulation (GDPR) and all laws concerning data of special categories 'make a fundamental conceptual mistake' when they focus on the nature of personal data: 'the borderlines of many categories are so blurry that they are useless'.[1] Instead, 'protections should be proportionate to the harm and risk' associated with the data processing. This Solove's article is intended as a contribution to the American debate over whether to adopt national privacy laws using an approach similar to that of the GDPR. However, it also takes a broader perspective – going beyond just the issue of special categories of data – and questions the very definition of personal data itself. In our opinion, this proposal also has value in contributing to the discussion on the jurisprudence of the Court of Justice of the European Union (CJEU).

The expansion of the notion of data of special categories has already been observed by many European scholars. Indeed, the CJEU has acknowledged some cases where special categories of data can be inferred, which, according to Solove, is one reason the boundaries between categories have become blurred.[2] Moreover, including data of special categories within the scope of the right to be forgotten has also contributed to the broadening of the notion. On the other hand, one of the most sensitive types of data – health data – has also drawn attention from a consumer protection perspective: as a result, even competing companies have sometimes been allowed to protect third-party' data of special categories. The final emerging trend for data of special categories originates from recent CJEU rulings involving social networks.

However, the expansion of sensitive data does not, *per se*, lead to Solove's conclusion that special categories are conceptually useless. For example,

[1] D Solove, 'Data is what data does. Regulating based on harm and risk instead of sensitive data' (2024) 118(4) Northwestern University Law Review 1081–1083. On the contrary, the Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR issued by the European Data Protection Board (Version 1.0, adopted on 8 October 2024) still focus on the nature of data, stating that 'the more sensitive or private the nature of the data to be processed, the more likely it is that the processing of such data will have a negative impact on the data subject'.

[2] ibid 1099.

enhanced protection for sensitive data remains valuable where such data is published in databases or newspapers.

That said, there may be a need for a complementary approach – one grounded in the assessment of risk or harm – beyond the literal interpretation of Article 9 of the GDPR. Considering the range of special categories listed in Article 9 and the even longer list of exceptions, this paper [merely] seeks to contribute to the broader, collective discussion on the future of special categories of data and their effective regulation.

For this purpose, we begin by analysing the CJEU cases in which the scope of special categories has been extended beyond the textual limits of Article 9 GDPR through inference, the right to be forgotten, and the consumer protection and social network context. Our aim is to determine whether the concept of special categories remains coherent, or whether it has, in practice, been gradually replaced by a broader risk-based approach (Section 2). If the latter is true, it would lend strong support to Solove's concerns. Then, we examine the limits of this heightened category of personal data (Section 3). In this regard, the existence of a high risk of discrimination and harm in big data analytics that current jurisprudence may not adequately address could be a strong reason to revisit the scope and content of Article 9 GDPR, or even to reconsider the continued usefulness of the notion of special categories of data altogether. Lastly, we will offer our conclusions (Section 4).

2. The limited and selective expansion of the notion of data of special categories in the CJEU jurisprudence.

In this section, we analyse how the CJEU has expanded the notion of sensitive data in three contexts: through inference (2.1), in relation to the right to be forgotten (2.2), and within the framework of competition law and social networks (2.3).

2.1. The limited acceptance of inference in CJEU jurisprudence.

Melissa Stock's comment on CJEU Case Vyriausioji tarnybinės etikos komisija (C-184/20)[3] clearly highlighted the expansion of the prohibition of processing of data of special categories to include inferred data.[4] In Lithuania, all public officers, as well as employees of non-governmental organisations, are required to declare their private data, including their name, personal identification number, social security number, income from self-employment, certain financial transactions, and any conflicts of interest. The same information must also be declared in relation to their spouse, cohabitee, or partner. Although most of this information is not published on the website of the Chief Official Ethics Commission, the name of the spouse, cohabitee, or partner is publicly available. As a result, the sexual orientation of the declarant and their partner

[3] Judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601.
[4] M Stock, 'Case Comment: The CJEU Expands the Scope of the Definition of Sensitive Personal Data in the GDPR: Case C-184/20 Vyriausioji tarnybinės etikos komisija' (2023) 24(1) Business Law International 93.

may be inferred from this data. The public disclosure of this information, though not being an explicit indication of a person's sexual orientation, was not strictly necessary and found to breach the principle of data minimisation. Moreover, publishing the name of a declarant's spouse, partner, or cohabitee exposes them to targeted advertising, commercial solicitation, or even criminal activity.

Therefore, the words 'revealing' and 'concerning', used to describe the prohibitions in Article 9(1) GDPR, [5] have been interpreted to include the inference of the information about sexual orientation from non-sensitive personal data – in this case, a partner's name: 'a wide interpretation of the terms 'special categories of personal data' and 'sensitive data' is confirmed by the objective of Directive 95/46 and the GDPR, (…) which is to ensure a high level of protection of the fundamental rights'.[6] Therefore, 'those provisions cannot be interpreted as meaning that the processing of personal data that are [leading] indirectly to reveal sensitive information concerning a natural person is excluded from the strengthened protection regime prescribed by those provisions'. [7] A broader perspective seems to emerge from this reasoning, particularly when considering how big data, machine learning (ML), or artificial intelligence (AI) may facilitate the inference of a 'hidden layer' of sensitive data and could blur the boundary between ordinary personal data and sensitive data,[8] as we will analyse in Section 3. These authors suggest that the nature of the processing, the objective suitability of the processed data for deriving the 'hidden layer', and the context-dependent sensitivity of the data should be taken into account.

However, the Court does not make any general statement regarding the broader applicability of this inference-based expansion, nor does it clearly define its consequences. Therefore, the Decision rather appears to represent an exception, limited in scope, and specifically applicable to non-public servants.[9] According to Hoppe, the different level of privacy protection in the CJEU Case Vyriausioji tarnybinės etikos komisija (C-184/20) as opposed to previous Decisions of the European Court of Human Rights (ECtHR), that were not even mentioned in the former Case, arises from the CJEU's finding that the

[5] Article 9.1 GDPR prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. There are some exceptions (Article 9(2)) that permit the processing of sensitive data: explicit consent (a); necessity for employment and social security purposes (b); protection of the vital interests of the data subject or of another natural person (c); legitimate activities by a foundation and similar bodies (d); related to personal data which are manifestly made public by the data subject (e); necessity for the establishment, exercise or defence of legal claims (f); necessity for reasons of substantial public interest, on the basis of union or Member State law (g); necessity for medicinal purposes or for the management of health systems and services (h); necessity for reasons of public interest in the area of public health (i); necessity for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (j).

[6] Judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601, paragraph 125.

[7] ibid § 126.

[8] M Matejek and S Kremer, 'Sensible Daten soweit das Auge reicht: Der EuGH zapft den 'hidden layer' an' (2023) 4 Daten und Sicherheit 218.

[9] T Hoppe, 'Anticorruption, Privacy, and (Gay) Family – The CJEU Rules on Financial Disclosure of Public Officials (C-184/20)' (2013)17(4) ICL Journal 433–446.

declarant was not a public servant.[10] The Lithuanian law indeed treats the heads of NGOs receiving public funds as public servants, but the CJEU did not. This highlights, once again, the limited scope of this inference-based expansion: its applicability depends on the specific circumstances and is subject to the proportionality test (article 9(2) g) GDPR), on a case-by-case basis. If the country allows same-gender relationships, public officers could legitimately declare their partners to an agency monitoring asset declarations, but its public disclosure would require previous consent. In homophobic environments, the declaration and collection of this information from public authorities could contribute to discrimination on the ground of sexual orientation, no matter whether the declarant holds a public or a private position.[11]

2.2 The right to be forgotten: a latent generalisable expansion of special categories of data via the balancing test of Article 9(2)g) GDPR, and upon request.

The CJEU did not address the processing of sensitive personal data by search engine operators in its seminal Decision on the right to be forgotten, also known as the right to erasure or de-referencing, in Google Spain and Google (Case C-131/12).[12] The question was later answered in GC and Others (C-136/17), where the Court held there is no general prohibition on the processing of sensitive personal data by search engine operators.[13] Indeed, such operators may lawfully process sensitive data, even in the absence of a relevant exception under Article 9(2) GDPR, provided that the data subject does not object. Consequently, the level of protection afforded to sensitive data is effectively reduced unless the data subject actively asserts their rights.[14] Nonetheless, this creates a practical framework for search engine operators. The exceptions allowing them to process sensitive data could be: explicit consent (Art. 9(2) a) GDPR), which is rarely practical in this case; the data being manifestly made public by the data subject, though this exception was not cited in the Decision; and, almost notably, processing for reasons of substantial public interest (Art. 9(2) g) GDPR. Specifically, the Court mentions the right of freedom of information for Internet users (Art. 11 of the Charter of Fundamental Rights of the European Union).

The expansion of the notion of special categories of data in the context of search engine operators is, thus, based on a balancing of the right to data protection with the freedom of information, mainly, but not exclusively, in relation to journalistic content. Even where no explicit legal ground for personal data processing applies and the principles of Article 5 GDPR are not fully respected, the processing of sensitive data by search engines may still be

[10] Previous related Cases non mentioned in Case C-184/20 are *Wypych v Poland* (dec.), no. 2428/05, ECtHR 2005 and *Xhoxhaj v Albania*, no. 15227/19, ECtHR 2021.
[11] Hoppe, *Anticorruption, Privacy and (Gay) Family* (n 9).
[12] Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317.
[13] Judgment of 24 September 2019, *GC and Others,* C-136/17, EU:C:2019:773.
[14] J Globocnik 'The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)' (2020) 69(4) GRUR International 380–388.

deemed lawful if the balancing exercise favours it.[15] This assessment is explicitly tailored to search engine operators, but its rationale is potentially generalisable to other similar scenarios where there is no possibility to operate an *ex ante* and systematic control over the data to be processed, such as web scraping[16] or development and training of AI models.

The Court has therefore not established a blanket prohibition of the processing of sensitive personal data by search engine operators. Instead, they will have to monitor the processing *ex post* and decide, using a balancing of rights upon data subject's request and on a case-by-case basis, whether it is allowed or not to process the sensitive data. This approach may well extend to similar future cases, beyond search engines; though, its potential awaits further clarification in subsequent decisions of the CJEU.

2.3 A potential game-changer: protecting data of special categories on social networks through competition law.

The most recent expansive CJEU jurisprudence on special categories of data relates to social networks and competition law. Two leading cases need to be considered for this purpose: Meta Platforms and others (C-252/21) and Schrems (C-446/21).[17]

In the Case Meta Platforms and others, the CJEU held that a competition authority may consider data protection infringements when assessing abuse of a dominant position, pursuant to Article 102 TFUE, provided such consideration is necessary to establish the abuse. Competition authorities may require collaboration of national data protection authorities and must always follow their jurisprudence. As such, this opens the door to strengthening the protection of sensitive data when dealing with digital economy companies, such as social networks. Indeed, processing of personal data by an online social network may be prohibited when it reveals any of the sensitive categories listed in Article 9(1) GDPR, subject to derogations of Article 9(2) GDPR, irrespective of whether the information is accurate or whether the controller intends to obtain it.[18] Visiting websites or apps in certain cases may indirectly reveal such information without explicit disclosure by the data subject, thus constituting the processing of sensitive data.

The derogation under Article 9(2) e) GDPR requires an explicit and clear action by the data subject to make the data accessible to the public. When visiting websites or apps that may reveal sensitive information, users do not necessarily intend to make such information public; at most, such data might be intended for the website or app operator. Moreover, interactions via 'like' or 'share' buttons are governed by user-specific settings, and public disclosure to unlimited number of people requires explicit consent on specific individual setting in this sense. On the other hand, if the collected data set contains both

[15] Judgment of 24 September 2019, *GC and Others*, C-136/17, EU:C:2019:773, paragraph 75.
[16] Globocnik, *The Right to Be Forgotten* (n 14) 387.
[17] Judgment of 4 July 2023, *Meta Platform and others*, C-252/21, EU:C:2023:537.
[18] ibid §§ 66–69.

sensitive and non-sensitive data and no derogation under Article 9(2) GDPR applies, the general prohibition of Article 9(1) GDPR remains in effect.

Another example of the protection of special categories of data in social networks is the Case Schrems (C-446/21).[19] This Case is another opportunity for the Court to revisit its previous jurisprudence of Meta Platforms and others (C-252/21). Specifically, Article 9(2) e) GDPR is revisited as exception in the contexts of a user openly discussing their sexual orientation during a panel discussion. Although the data subject manifestly made this information public, the Court ruled that this alone does not permit the social network operator to process all other data related to that person's sexual orientation – such as data gathered from third-party websites and apps – for the purposes of delivering personalised advertisements.

In summary, this line of jurisprudence offers a more substantial expansion of the protection of special categories of data than previous developments. In sharp contrast with the Third-Party Doctrine in the USA, the CJEU does not treat social networks as public spaces, where users lose all expectation of privacy. Nor does it treat them as private spaces, where a reasonable expectation of data protection would generally exist. Rather, a nuanced approach is preferred and, in certain cases, specific and explicit consent is required for public disclosure, and the threshold for this consent remains high.

3. The limits of the notion of data of special categories.

While in the previous section we have analysed how the CJEU has extended the notion of data of special categories in various contexts, in this section, we explore the limitations that this notion presents as currently interpreted by the Court.

In the field of AI, it has been argued that the strengthened protection regime envisaged for data of special categories under the GDPR might be insufficient to address AI's discriminatory impacts or its implications for individuals' privacy and reputation. We analyse how this regime, as interpreted by the CJEU, may fail to provide an adequate protection standard in the context of big data analytics (3.1). Then, we study how, assuming that all personal data has the potential to become sensitive challenges the GDPR's protection of special categories of data limits the possibility of relying on legitimate interest as a legal basis for development and training of AI models (3.2).

3.1 Inferences of data of special categories in big data analytics.

It has been questioned whether the categorisation of sensitive data is useful in big data analytics. As Williams *et al.* explain, big data is composed of densely packed traces of individuals' lives pieced. Within such datasets, certain personal characteristics frequently appear together ('correlations' or 'patterns'). [20]

[19] Judgment of 4 October 2024, *Schrems*, C-446/21, EU:C:2024:834.
[20] BA Williams and others, 'How Algorithms Discriminate Based on Data they Lack: Challenges, Solutions, and Policy Implications' (2018) 8 Journal of Information Policy 78–115.

These patterns may exist within a single individual's data (e.g. tennis class every Thursday), or across groups (e.g. residents of a certain neighbourhood tending to pay rent late). AI and ML systems can analyse these datasets, structure the data and create detailed individual profiles that necessarily include highly sensitive information. It is not necessary for sensitive data to be present *per se* in these datasets; such data may be inferred (directly or through the combination of personal or non-personal data).

The ECtHR Guide on its case law regarding data protection warns that there are categories of personal data other than those categorised as sensitive data that are also of concern 'especially with the increasingly sophisticated surveillance techniques and the capacity of information and communication technologies to make the daily life of data subjects more difficult'. [21] This remark questions the usefulness of any *numerus clausus* list of sensitive data categories. In this regard, it is unclear why the categories of data listed in Article 9 GDPR are considered special and other data, such as sex, social class, IP address or home address, is not.[22] The envisaged special categories do not align precisely with the protected grounds of the European Union (EU) antidiscrimination directives (sex, racial or ethnic origin, sexual orientation, religion or belief, age, or disability). The CJEU in the Case Meta Platforms and Others (C-252/21) specifies that data should be considered sensitive if such data allows for the inference of information falling within one of the categories listed in Article 9(1) GDPR. [23] Consequently, information revealing other characteristics (e.g. data revealing sex, economic or labour situation) that are not specified in Article 9 GDPR (but may equally have discriminatory impact or implications for privacy or reputation) falls outside the scope of special categories.

To this end, geo-location or browsing history can be used to draw precise conclusions about people's private live, such as daily routines or permanent or temporary residence. [24] Furthermore, nearly all apps make use of highly sensitive and personally identifiable information.[25] Such a massive volume of data increases risks of discrimination, exposure of sensitive information, and privacy violations. Within this context, the interplay between Article 9 GDPR and big data analytics becomes complex.

Quinn and Malgieri explain this challenge in the following terms: if only data listed in Article 9 GDPR is considered sensitive, other data can be used to deduce the same protected information. Conversely, if all data that can indirectly reveal sensitive information is considered sensitive, then nearly all

[21] ECtHR, Guide to the Case-Law of the European Court of Human Rights, Data protection, 31 December 2020, Updated on 31 August 2024. Available in <https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_eng>, 15.
[22] Solove, 'Data is what data does.' (n 1) 1086.
[23] Judgment of 4 July 2023, *Meta Platform and others*, C-252/21, EU:C:2023:537, paragraph 68.
[24] JA Huerta Anguiano '"Naturaleza intrínseca", "contexto" o "finalidad" en la determinación del carácter sensible de los datos personales' (2020) 1(10) Estudios En Derecho a La Información 1–31.
[25] AS Devi and A Chinnasamy, 'Privacy Preservation of sensitive data in big data analytics – A survey' (2021) 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON), 1–5.

personal data could fall within the scope of special categories of data, particularly given the combinatorial power of big data analytics.[26]

In the case Meta Platforms and Others (C-252/21), the CJEU stated that the processing of a dataset is prohibited if it is impossible to isolate non-sensitive data from sensitive data items at the time of collection. The Court refers to the occasions where the dataset contains at least one sensitive data item (see Section 2.3).

What does the CJEU mean when referring to 'sensitive data item'? As we referenced in Section 2.1, in the Case Vyriausioji tarnybinės etikos komisija (C-184/20), the Court asserts that information indirectly revealing sensitive information falls within the scope of Article 9 GDPR.[27] Advocate General Pikamäe affirms in his Opinion on the Case that the use of the verb 'reveal' includes an intellectual exercise involving deduction or cross-referencing.[28] Moreover, the Article 29 Working Parity (A29WP) further clarifies that the term 'data revealing' includes not only inherently sensitive data, but also such data from which sensitive information regarding an individual may be inferred.[29] As a result, it can be argued that inferred sensitive data, which is common in big data analytics,[30] should also receive heightened protection.

Nevertheless, as we previously pointed out, the Decision in Vyriausioji tarnybinės etikos komisija (C-184/20) seems exceptional, and later judgments indicate that the CJEU has not further extended this doctrine to big data analytics when stated the expansion of this principle regarding the inference in this Case. In this sense, it can be questioned whether the mechanism of 'separat[ing] the data items from each other at the time of collection'[31] referred in the Meta Platform and others (C-252/21) judgement is feasible in big data analytics. Van de Waerdt argues that this judgement reaffirms traditional principles of the data protection legislation in an unambiguous way and may have serious implications for digital market companies, which are likely to process (accidentally or not) special categories of data regarding their users given their widespread data collection.[32] Solove highlights that the idea that special categories of data can be separated is impractical in big data settings, where most of personal data is interconnected and may be inferred by algorithms.[33] Malgieri and Comandé argue that the identification of sensitive data can be difficult in the world of undisclosed algorithms and machine-generated inferences and predictions, where even the controllers

[26] P Quinn and G Malgieri, 'The Difficulty of Defining Sensitive Data–The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22(8) German Law Journal 1583.
[27] ibid § 127.
[28] Opinion of Advocate General Pikamäe in the CJEU case *Vyriausioji tarnybinės etikos komisija* (C-184/20), delivered on 9 December 2021, EU:C:2021:991, paragraph 85.
[29] Article 29 Data Protection Working Party, Advice Paper on Special Categories of Data ('Sensitive Data'), 4th April 2011, Ref. Ares ((2011)444105-20/04/2011).
[30] The European Data Protection Board Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024, does not analyse the processing of special categories of data in AI models (§ 17).
[31] Judgment of 4 July 2023, *Meta Platform and others*, C-252/21, EU:C:2023:537, paragraph 89.
[32] PJ van de Waerdt, 'Meta v Bundeskartellamt: Something Old, Something New' 8(3) European Papers: A journal on law and integration 1077.
[33] Solove, 'Data is what data does.' (n 1) 1083.

themselves may not be able to identify such data. [34] In particular, the identification of sensitive data can be difficult if the results given by the AI system are not human-readable.

In this regard, and taking into account that operating an *ex ante* and systematic control of what data will be processed seems to be difficult, it may be appropriate to extend the doctrine established by the CJEU Case GC and others (C-136/17) to big data analytics: data could be lawfully processed to develop and train AI models – even without an applicable exception under Article 9(2) GDPR – unless the data subject actively exercise their rights.

Alternative solutions have been proposed by the legal scholars to address the problem of the effectiveness of the GDPR's current model in light of the inference of sensitive data from other data. Nissenbaum suggests that categorising data as sensitive should be based on the context of the processing. [35] Purtova proposes that personal data should be protected according to potential individual or public negative consequences of the data processing. [36] Lastly, Quinn and Malgieri argue that data should only be considered sensitive if the 'intention of the data controller is to process or uncover sensitive information or if it is reasonably foreseeable that, in a given context, the data in question could be used to reveal or to infer sensitive aspects of data subjects'.[37]

In relation to this last proposal, the intention qualifier does not seem to be a suitable solution in big data scenarios, since it can be difficult or impossible to prove. As an example, in anti-discrimination law, there is a phenomenon called 'masking', that can be described as intentional discrimination disguised through technical opacity and complexity as unintentional discrimination.[38]

Furthermore, as we referenced in Section 2.3, the CJEU in the Case Meta Platforms and Others (C-252/21), states that it is irrelevant whether the information revealed by the processing operation in question is accurate, or whether the controller is acting with the aim of obtaining information that falls within one of the special categories.[39]

Fabris *et al.* argue that special categories of data are infrequent and difficult to process, hence limiting fairness approaches to proxy reduction or removal[40] (enabled by Article 10(5) AI Act).[41] The authors propose that the EU AI Act's

---

[34] G Malgieri and G Comandé, 'Sensitive-by-distance: quasi-health data in the algorithmic era' (2017) 26(3) Information and Communications Technology Law 229.

[35] H Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009).

[36] N Purtova, 'The law of everything: Broad concept of personal data and future of EU data protection law' (2018) 10(1) Law, Innovation and Technology 40. The author highlights that the rapid progress of (re)identification technologies and failure of anonymisation play an important role in the argument that everything will soon fall within the definition of personal data (any information relating to an identified or identifiable natural person) as interpreted by the A29WP and the CJEU.

[37] Quinn and Malgieri, *The Difficulty of Defining Sensitive Data* (n 26) 1612.

[38] JA Kroll and others, 'Accountable Algorithms' (2017) 165(3) U. Pa. L. Rev. 633–705.

[39] Judgment of 4 July 2023, *Meta Platform and others*, C-252/21, EU:C:2023:537, paragraph 69.

[40] A Fabris and others, 'Fairness and Bias in Algorithmic Hiring: A Multidisciplinary Survey' (2025) 16 ACM Trans. Intell. Syst. Technol 1, 40.

[41] This Article provides another exception to allow the processing of sensitive data. The Article enables providers of high-risk AI systems to exceptionally process special categories of personal data when strictly necessary for the purpose of ensuring bias detection and correction, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. Certain conditions for the processing must be met: the same purpose cannot be effectively fulfilled by processing other data (a); technical limitations are

exception to Article 9(1) GDPR be expanded to cover other scenarios where processing of special categories of data is necessary to prevent violations of certain rights of the data subjects (e.g. non-discrimination, privacy).

In summary, if the CJEU expands the notion of special categories of data to big data analytics, and a harm or risk-based approach is adopted, the concept of sensitive data may effectively collapse, considering that all personal and non-personal data in big data analytics may become sensitive information in a fraction of a second.[42] The absence of a clear regulatory framework for what constitutes sensitive data, especially in the context of big data analytics, can have further implications, as we address in the following section.

3.2 Special-category data, legitimate interest and AI model training.

An issue that arises from the ambiguous protection of inferred sensitive data in big data analytics is that, depending on what data is considered sensitive, the training and development of AI models may be either permitted or prohibited. The lack of guidance from the CJEU jurisprudence has resulted in limitations on the protection that can be derived from the concept of special categories of data.

AI systems, particularly those based on ML, require the use of data during the training phase, prior to being applied to new data in the operational phase. Based on this distinction, the Commission Nationale de l'Informatique et des Libertés (CNIL) issued a guideline on artificial intelligence,[43] stating that the processing of personal data for training purposes is subject to the GDPR if the training phase is separated from the operational implementation of the AI system and its sole purpose is to develop or improve the performance of the AI system.

The Belgian Data Protection Authority, in the Decision 46/2024 of 15th March,[44] also stated that it was necessary to distinguish between the stage of creating or training the AI model itself, and the operational stage, in which personalised discounts were offered through the digital applications that utilised the models created during the previous stage.[45] In that case, the claimant argued that the defendant (a bank) was using costumer transaction data to create and train AI models for offering personalised discounts for third-party products and services – thus processing data for a purpose different from the original one (executing and recording transactions).[46] The defendant

implemented in relation to the reuse of the data (b); measures are implemented to avoid misuse and ensure that only authorised persons have access to the data (c); data is not transmitted, transferred or accessed by other parties (d); data is deleted once the bias is corrected or the retention period has reached the end (e); and a record of the processing activities is performed, including why it was strictly necessary and why the purpose could not be achieved by processing other data.

[42] B van der Sloot, 'Regulating non-personal data in the age of Big Data', in M Tzanou (ed.), *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (Routledge 2020) 85.

[43] Commission Nationale de l'Informatique et des Libertés (CNIL), AI: ensuring GDPR compliance (21st September 2022). Available at: <https://www.cnil.fr/en/ai-ensuring-gdpr-compliance>.

[44] Autorité de protection des données, Décision quant au fond 46/2024 du 15 mars 2024, Numéro de dossier: DOS-2019-05837. Available in: <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n0-46-2024.pdf>.

[45] ibid § 45.

[46] ibid § 26.

argued that the legal basis for the processing of personal data at the training stage was legitimate interest (requiring that data subjects be informed and not object), and the legal basis for the operational stage was explicit consent (requiring that data subjects explicitly consent).[47] The Data Protection Authority accepted the defendant's argument regarding the distinction between two stages (training and operation) of the AI model and the use of legitimate interest as a legal basis for the training phase. Korff asserts, on the contrary, that the purpose of both stages was the same – direct marketing – and therefore the creation and training of the model (stage one) cannot be viewed as an independent activity,[48] since the two stages had the same purpose.[49]

Using this example as a reference, it is reasonable to question whether distinguishing the creation and training of AI models, on the one hand, and their operational use, on the other, has implications for the protection (and the usefulness of the classification) of special categories of personal data.

Under the GDPR, for data processing to be lawful, the processing must rely on one of the lawful grounds listed in Article 6 for non-sensitive personal data, and one of the additional grounds provided in Article 9 if special categories of data are involved.[50] The controller must satisfy the requirements of both GDPR provisions (Article 6 and Article 9) when it processes special categories of personal data.[51] Subsequently, processing of sensitive data is only allowed when one of the specific additional conditions set out in Article 9(2) GDPR applies.

The issue, therefore, remains the following: if the AI model is created and trained by processing non-sensitive personal data, legitimate interest may serve as an appropriate legal basis, provided that data subjects are informed and not object.[52] Alternatively, if sensitive personal data was used during the creation and training of the AI model, legitimate interest alone cannot be sufficient: an exception from Article 9(2) must apply, and data subjects must be informed.[53]

---

[47] ibid § 45.

[48] D Korff, 'Applying the EU General Data Protection Regulation (GDPR) to the use of personal data to train an AI system: A follow-up to my note on a deeply defective and flawed Belgian decision' (2024a). Blog [Data protection and digital competition].

[49] This case would be different for General Purpose AI Models (regulated in Chapter V of the AI Act) because the creating and training of the AI model can serve a *variety of purposes* both for direct use as well as for integration in other AI systems (Article 3.66 AI Act).

[50] European Union Agency for Fundamental Rights, Hand- book on European data protection law 2018 edition (2018), § 117. Available at: <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>.

[51] The European Data Protection Board Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024, does not analyse the processing of special categories of data in AI models (footnote 47).

[52] Korff argues that 'legitimate interest' can only be relied on if it is considered that there is sensitive data in the dataset when the sensitive data: a) relates to members and "'close contacts' of political, philosophical, religious or trade union bodies and are only processed by those bodies; b) has been 'manifestly' made public by the data subject; or c) is (strictly) necessary in a legal claims context. See: D Korff, 'The legal bases for processing of non-sensitive and sensitive data including the 'legitimate interest' legal basis & the use of personal data to 'train' an AI model' (2024b). Blog [Data protection and digital competition].

[53] Korff, 'Applying the EU General Data Protection Regulation (GDPR) to the use of personal data to train an AI system' (n 48).

Considering the previously mentioned legal doctrine that claims that all datasets used in big data analytics contain sensitive data, legitimate interest (Article 6.1.f) can only be invoked for the creation and training AI models if an exception of Article 9(2) also applies.[54] As the CJEU pointed out in Meta Platforms and Others (C-252/21), if the dataset [e.g. used to create and train AI models] contains 'at least one sensitive data item', and none of the exceptions in Article 9(2) GDPR apply, the processing is prohibited.[55]

Alternatively, Velli suggests that legitimate interest 'appears especially relevant in the context of AI models in which there is no direct relationship between the data subjects and the controller'.[56] Likewise, Trigo Kramcsák considers that the legitimate interests pursued by the data controller or a third party emerge as a lawful ground for building AI and ML training datasets.[57] Despite acknowledging that the use of sensitive data during the training of AI models can be challenging (for relying on legitimate interest), the author concludes that it remains a viable option, given that 'AI models trained on inaccurate or biased data can lead to harmful outcomes for individuals'.[58] Another possible option, as previously discussed, would be to extrapolate from the CJEU doctrine in GC and others (C-136/17) and rely on 'reasons of substantial public interest' as a legal basis (Article 9(2) g) GDPR). In any case, all these interpretations imply a weakening of the protection granted to sensitive data when used in AI model training.

4. Conclusions.

We have described a limited and selective expansion of the notion of special categories of data in the jurisprudence of the CJEU. Inferred data has been included (not universally, but in the specific case examined) within the scope of the prohibition of processing of special categories of data. This expansion has also been studied in relation to the right to be forgotten, though it remains constrained by the need to balance competing rights and, almost notably, is typically triggered by a request from the data subject. Lastly, the considerations related to social networks and competition law may also contribute to extending the protection of special categories of data in public spaces.

Solove's concerns appear, therefore, unjustified, at least under the current implementations of the AI Act and the GDPR. However, this could change with the rise of big data analytics. Without broader recognition of the inference in respect of sensitive data, we are still far from achieving a reasonable expectation of protection for special categories of data in public spaces.

Additionally, there are several other reasons to remain concerned about the future of the concept of special categories of data: the blurring line between

[54] ibid.
[55] Judgment of 4 July 2023, *Meta Platform and others*, C-252/21, EU:C:2023:537, paragraph 89.
[56] F Velli 'Processing Personal Data in the Context of AI Models: EDPB's Opinion 28/2024' (2024) 9(3) European Papers: A journal on law and integration 1497, 1498.
[57] P Trigo Kramcsák, 'Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?' (2023) 48 CLSR 1, 11.
[58] ibid 11.

special categories of data and ordinary personal data, the reliance on the nature of data to determine whether it is considered sensitive, and the growing academic support for allowing the use of legitimate interest as a legal bases for training AI models.

However, shifting from fixed special categories of data towards a broader risk-based approach, as the AI Act proposes, may not be sufficient to adequately protect data users from discrimination and privacy harms, unless we recognise the existence of different kind of risks.

Capilli G, 'Some remarks on nanotechnologies, safety and product liability' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252GC

EJPLT
ISSN 2704-8012

Some remarks on nanotechnologies, safety and product liability

Alcune osservazioni su nanotecnologie, sicurezza e responsabilità da prodotto

GIOVANNA CAPILLI
Full professor of Private Law
Università San Raffaele di Roma

Abstract

This paper examines the legal implications of nanotechnology, focusing on consumer protection and product liability. It highlights how the precautionary principle guides regulatory and civil liability frameworks in managing scientific uncertainty and emerging risks. Emphasis is placed on transparency, labelling, and information disclosure as essential tools for informed consent and risk prevention taking into account the recent EU reforms, including the General Product Safety Regulation (EU) and the new Product Liability Directive (EU) 2024/2853. The study argues that precaution operates as a bridge between product safety regulation and civil liability, ensuring a dynamic balance between technological innovation and the protection of health, safety, and consumer trust in the nanotechnology era.

Il contributo analizza le implicazioni giuridiche delle nanotecnologie, con particolare attenzione alla tutela dei consumatori e alla responsabilità da prodotto. Si evidenzia come il principio di precauzione orienti i sistemi normativi e i modelli di responsabilità civile nella gestione dell'incertezza scientifica e dei rischi emergenti. L'analisi pone l'accento su trasparenza, etichettatura e divulgazione delle informazioni, considerate strumenti fondamentali per garantire il consenso informato e la prevenzione dei rischi, anche alla luce delle recenti riforme europee, tra cui il Regolamento (UE) sulla sicurezza generale dei prodotti e la nuova Direttiva (UE) 2024/2853 sulla responsabilità da prodotto. Lo studio sostiene che il principio di precauzione funge da ponte tra la regolamentazione della sicurezza dei prodotti e la responsabilità civile, assicurando un equilibrio dinamico tra innovazione tecnologica e tutela della salute, della sicurezza e della fiducia dei consumatori nell'era della nanotecnologia.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Nanotechnology; Precautionary Principle; Consumer Protection; Product Liability; Safety

Summary: 1. Benefits and Risks of Nanotechnologies. – 2. Consumer information in the Context of Nanotechnology Products. – 3. Producer Liability and the "Development Risk Defense" Clause. – 4. Burden of Proof (New Directive (EU) 2024/2853). – 5. Conclusion.

1. Benefits and Risks of Nanotechnologies.

The integration of nanotechnology into diverse sectors, including medicine, engineering, and consumer products,[1] has generated significant advancements and opportunities. At the same time, this rapid development raises important legal concerns, particularly with regard to liability and consumer protection.

A proper analysis must begin with a definition. Nanotechnology refers to the engineering, manipulation, and application of materials at the nanoscale (1–100 nm). It broadly encompasses any technology that incorporates engineered nanomaterials.[2]

Although these particles are exceedingly small, they pose substantial questions, as many of their interactions with the human body and the

[1] For example, it is possible to find nanotechnologies in refrigerator linings, in the house, in transport of food from producer to grocery store, in bicycle tires and cosmetics; other example in Swiss Nanocube, Nanorama: The World of Nanotechnology (Swiss Nanocube) http://www.swissnanocube.ch/nanorama/?L=3, accessed 6 October 2025, in which there is an interactive photos identify over fifty household items using nanotechnology and therefore representing potential exposure to engineered or manufactured nanoparticles in daily life.
A definition in European Chemicals Agency (ECHA), Nanomaterials https://echa.europa.eu/regulations/nanomaterials, accessed 6 October 2025: "Nanomaterials are chemical substances or materials with particle sizes between 1 to 100 nanometres in at least one dimension. Due to an increased specific surface area by volume, nanomaterials may have different characteristics compared to the same material without nanoscale features. As a result, the physicochemical properties of nanomaterials may differ from those of bulk substances or particles of a larger size. Many everyday products containing nanomaterials are already on the European market such as batteries, coatings, anti-bacterial clothing and cosmetics. While nanomaterials may offer technical and commercial opportunities, they may also pose risks to our health and the environment. Just like any other substance on the EU market, it is important to ensure that their uses are properly assessed and that any risks are adequately controlled"; see also Commission Recommendation of 10 June 2022 on the definition of nanomaterial: 'Nanomaterial' means a natural, incidental or manufactured material consisting of solid particles that are present, either on their own or as identifiable constituent particles in aggregates or agglomerates, and where 50 % or more of these particles in the number-based size distribution fulfil at least one of the following conditions:
(a) one or more external dimensions of the particle are in the size range 1 nm to 100 nm;
(b) the particle has an elongated shape, such as a rod, fibre or tube, where two external dimensions are smaller than 1 nm and the other dimension is larger than 100 nm;
(c) the particle has a plate-like shape, where one external dimension is smaller than 1 nm and the other dimensions are larger than 100 nm.
In the determination of the particle number-based size distribution, particles with at least two orthogonal external dimensions larger than 100 µm need not be considered.

[2] PC Binsfeld and JM Granjeiro, 'Nanotecnologias: regulação baseada em evidências' (2024) 12 Vigilância Sanitária em Debate https://doi.org/10.22239/2317-269X.02260, accessed 6 October 2025; JV McHale, 'Nanomedicine—Small Particles, Big Issues: A New Regulatory Dawn for Health Care Law and Bioethics?' in M Freeman (ed), *Law and Bioethics: Current Legal Issues*, vol 11 (Oxford University Press 2008; online edn, Oxford Academic, 1 Jan 2009) https://doi.org/10.1093/oso:acprof/9780199545520.003.0020, accessed 4 July 2025.

environment remain insufficiently understood.[3] Despite these uncertainties, products derived from nanomaterials – including food items[4] and packaging – are increasingly entering the consumer market.[5]

This situation brings to the forefront ethical, environmental, and safety challenges. Nanotechnologies and nanomaterials are not without risk. Indeed, the very characteristics that make nanoparticles valuable – such as their diminutive size, large surface-area-to-volume ratio, and high reactivity – may also generate unique and potentially hazardous effects on human health.

This paper examines the regulatory framework governing the use of nanotechnology with particular reference to the consumer protection and product liability.

This domain is strongly shaped by the precautionary principle, which requires proactive measures to prevent harm to public health and the environment even in the absence of complete scientific certainty. The principle highlights the importance of stringent regulatory standards and rigorous risk management practices in the development and deployment of nanotechnologies.

Moreover, this analysis emphasizes the essential role of information disclosure and product labelling in safeguarding consumers. Transparent and comprehensive labelling practices are vital for informing consumers about the presence and potential risks of nanomaterials in products. Proper labelling not only facilitates risk management but also strengthens consumer trust and supports informed decision-making.

Given the broad range of applications for nanotechnologies, attention must be directed towards the specific regulatory frameworks applicable to different product categories.[6] This requires harmonization with general principles of product liability, thereby ensuring consistent and comprehensive legal coverage. The jurist's role is pivotal in navigating this complex regulatory landscape while aligning specialized provisions with overarching liability principles in order to address the distinctive issues raised by nanotechnology.

A particularly significant development is the adoption of the new General Product Safety Regulation (EU) 2023/988,[7] which strengthens consumer

---

[3] GBB Nhani and others, 'High-Tech Sustainable Beauty: Exploring Nanotechnology for the Development of Cosmetics Using Plant and Animal By-Products' (2024) 11 Cosmetics 112 <https://doi.org/10.3390/cosmetics11040112>, accessed 6 October 2025.

[4] With reference food see: Regulation (EU) 2015/2283 of the European Parliament and of the Council of 25 November 2015 on novel foods, amending Regulation (EU) No 1169/2011 and repealing Regulation (EC) No 258/97 and Commission Regulation (EC) No 1852/2001 [2015] OJ L327/1; EFSA Scientific Committee, More S and others, 'Guidance on risk assessment of nanomaterials to be applied in the food and feed chain: human and animal health' (2021) 19(8) EFSA Journal 6768 <https://doi.org/10.2903/j.efsa.2021.6768>, accessed 6 October 2025.

[5] More information in: European Commission, Opinion on Nanomaterials <https://ec.europa.eu/health/scientific_committees/opinions_layman/nanomaterials/en/l-2/1.html>, accessed 6 October 2025 "Current applications include healthcare (in targeted drug delivery, regenerative medicine, and diagnostics), electronics, cosmetics, textiles, information technology and environmental protection. For example, nanosilver is appearing in a range of products, including washing machines, socks, food packaging, wound dressings and food supplements".

[6] Cosmetics Regulation: Imposes specific safety requirements for nanoparticles in cosmetics. Main legislation: European Commission, Cosmetics Legislation Overview <https://single-market-economy.ec.europa.eu/sectors/cosmetics/legislation_en>, accessed 6 October 2025

[7] P Steindl, 'Consumer Neuro Devices within EU Product Safety Law: Are We Prepared for Big Tech ante Portas?' (2024) 52 Computer Law & Security Review 105945 <https://doi.org/10.1016/j.clsr.2024.105945>, accessed 6 October 2025.

protection by introducing enhanced mechanisms for identifying and managing emerging risks, including those arising from nanoscale substances. Legal professionals must critically assess how this Regulation interacts with existing legal frameworks and embodies the precautionary principle, thereby contributing to a more comprehensive and adaptive model of product safety.

In light of the transversal, disruptive, and pervasive nature of nanotechnologies, their regulation requires not only specialized scientific expertise but also a legal architecture capable of addressing their specific risk profiles. The nanoscale dimension of materials generates unprecedented challenges that demand tailored regulatory solutions, proactive governance strategies, and oversight mechanisms grounded in transparency, accountability, and risk prevention. The evolving character of nanotechnologies therefore calls for a dynamic and responsive legal framework that balances innovation with the protection of public health and the environment.

2. Consumer information in the Context of Nanotechnology Products.

Consumer information constitutes a fundamental component of health and safety protection, particularly in the context of emerging technologies such as nanotechnology. The principle of the "right to know" is a cornerstone of informed consent and plays a crucial role in safeguarding both public and consumer health. Furthermore, it serves to mitigate potential legal liability for businesses engaged in the development and application of nanotechnology. [8]

A major legal and regulatory challenge in this domain lies in the persistent scientific uncertainty and the absence of reliable, reproducible data concerning potential risks. [9] These deficiencies directly hinder the application of two core components of informed consent: (i) the obligation to disclose known risks in a manner that enables the consumer or end-user to make an informed choice; and (ii) the subsequent acceptance of such risks – i.e., the provision of consent despite awareness of those risks – based on robust and validated scientific evidence.

In the case of nanotechnology, these requirements cannot presently be fulfilled due to the limited state of scientific knowledge, particularly with respect to cumulative, long-term, and unquantifiable risks arising from prolonged exposure. This evidentiary gap raises significant concerns in several areas of legal and ethical significance, including consumer protection (especially in biomedical and nanomedical applications), patient safety, nanosafety, and potential corporate liability. In the absence of sufficient data,

[8] Committee on Social Affairs, Health and Sustainable Development, Nanotechnology: Balancing Benefits and Risks to Public Health and the Environment, Rapporteur: Valeriy Sudarenkov, Russian Federation, SOCAS/Soc/Inf (2013) 03.

[9] B Pastore, 'Tecnologie emergenti, incertezze della scienza, regolamentazione giuridica' (2020) 2(17) Teoria e Critica della Regolazione Sociale / Theory and Criticism of Social Regulation 97 <https://mimesisjournals.com/ojs/index.php/tcrs/article/view/63>, accessed 18 July 2025.

ensuring regulatory compliance and mitigating liability for manufacturers and healthcare providers remain highly problematic. [10]

Traditional mechanisms of informed consent - such as those embedded in REACH and the Prior Informed Consent (PIC) procedure - [11] prove difficult to implement effectively. [12]

These frameworks presume that producers disclose known risks, thereby enabling consumers, including corporate actors, to make informed choices. Such disclosure functions as a liability shield, based on the assumption that risk is knowingly accepted by the informed party. Yet, in the context of nanotechnology, the paucity of validated scientific data undermines both the adequacy and comprehensibility of disclosures, raising serious bioethical and legal concerns.

Key issues include: (1) the consumer's capacity to comprehend technical risk disclosures; (2) the sufficiency and quality of such disclosures to support meaningful consent; and (3) the scientific reliability of the underlying data. Within REACH, consumers have the "right to know" (see article 33) whether the products they purchase contain hazardous chemicals. However, in this field the precautionary principle becomes essential to bridging the gap between scientific uncertainty and the legal requirement of informed consent, pending the establishment of a robust evidentiary baseline.

The precautionary principle operates as a legal tool for managing risks that remain unidentified or insufficiently characterised.[13]

The precautionary approach – distinct from the notion of anticipatory preventive action – requires that, in conditions of scientific uncertainty, the conduct of the entrepreneur or producer be guided by prudence, with a view to prioritizing safety over risk. From a legal standpoint, a further consideration warrants closer examination.

---

[10] Committee on Social Affairs, Health and Sustainable Development, Nanotechnology: Balancing Benefits and Risks to Public Health and the Environment, Rapporteur: Valeriy Sudarenkov, Russian Federation, SOCAS/Soc/Inf (2013) 03.

[11] More information at European Commission, REACH Regulation – Chemicals and Nanomaterials <https://environment.ec.europa.eu/topics/chemicals/reach-regulation_en>, accessed 6 October 2025 in which it can read: Nanomaterials are chemical substances or materials comprising very small particles of different shapes and sizes no larger than 100 nm. Many occur in nature, but most have been engineered to exhibit novel characteristics such as increased strength, chemical reactivity or conductivity compared to their non-nano counterparts. The REACH Regulation initially made no specific provision for nanomaterials. In 2018 the Commission adopted Commission Regulation (EU) 2018/1881 to modify REACH technical Annexes I, III and VI-XII, introducing nano-specific clarifications and provisions. In 2020 the Commission also updated Annex II with Commission Regulation (EU) 2020/878, introducing new provisions on Safety Data Sheets to complement the new registration requirements for nanomaterials. In 2011 the Commission adopted the Recommendation on the definition of a nanomaterial. This definition has informed many EU directives and regulations and has been supported by implementation guidance. The Recommendation was reviewed and revised in 2022 retaining its principal features. Supplemental information about the revised Recommendation has been provided by the Industrial Minerals Association (IMA) and the Germany Federal Institute for Risk Assessment (BfR).

[12] AskREACH, Art. 33 REACH: A Right to Know, Not a Right to Ask – Final Conference <https://www.askreach.eu/art-33-reach-a-right-to-know-not-a-right-to-ask-final-conference-takes-stock-after-more-than-5-years/> accessed 6 October 2025

[13] G Capilli, 'Gli obblighi di precauzione dell'impresa' in G Alpa and G Conte (eds), *La responsabilità di impresa* (Giuffrè 2015) 149–189; E Al Mureden, *Principio di precauzione, tutela della salute e responsabilità civile*, (Libreria Bonomo 2008); G Alpa, 'Responsabilità d'impresa', in *Digesto delle discipline privatistiche – Sezione Civile*, aggiornamento (UTET 2014) 560 ff.; G Comandè, 'La responsabilità civile per danno da prodotto difettoso… assunta con "precauzione"' (2013) 1 Danno e Responsabilità 107.

The assessment of product safety is therefore intrinsically linked to the nature of the product itself. This interplay between regulatory measures and consumer rights underscores the need for a nuanced approach to balancing innovation with safety. Particularly in the field of nanotechnology, the precautionary principle provides a critical framework for addressing the "unknown unknowns" inherent to nanoscale substances.

Equally, transparency and effective communication are indispensable. Labelling and information practices, as integral elements of informed consent, must be strengthened to ensure clarity and accessibility. This requires a collaborative effort among regulators, producers, and scientific communities to develop standardised guidelines capable of translating complex technical data into forms comprehensible to consumers. Such measures not only enable consumers to make informed choices but also mitigate liability risks for manufacturers by fostering trust and compliance in the marketplace.

Consequently, the precautionary conduct of producers must be calibrated in accordance with the specific category of product and the intended users or recipients.

This calls for a re-examination of the foundations of civil liability in light of the precautionary principle. Liability attribution rules play an evolving role in incentivizing virtuous conduct in risk management and accident prevention, adapting to technological and organisational developments within the relevant sector.[14]

Against this background, the revised Classification, Labelling and Packaging (CLP) Regulation, which entered into force on 10 December 2024, represents a significant step forward in protecting human health and the environment. At the same time, it strengthens the EU's internal market for chemicals, fostering a more competitive, transparent, and sustainable chemical industry.

Key improvements include clearer communication of chemical hazards – especially in online sales – through simplified and modernised labelling requirements. The new rules introduce flexible formats (such as fold-out and digital labels) and stricter standards of legibility. These changes are designed to make safety information more accessible and user-friendly for everyone. Another important feature is the requirement that advertisements and online product listings include clear hazard information. This will enable consumers to make more informed choices and support the growth of a market for sustainable chemical products. For the first time, the Regulation clarifies how household chemicals can be safely sold via refill stations, thereby reducing packaging waste and supporting environmentally sustainable consumption. Small and medium-sized enterprises (SMEs) will benefit from a streamlined and more user-friendly notification system. Overall, the revised CLP Regulation demonstrates a strong commitment to improving safety, enhancing transparency, and supporting innovation in the chemical sector, while keeping pace with new technologies and sustainability goals.[15]

[14] G Capilli, 'Gli obblighi di precauzione dell'impresa' in G Alpa and G Conte (eds), *La responsabilità di impresa* (Giuffrè 2015) 149–189.

[15] <https://environment.ec.europa.eu/news/revised-chemical-labelling-regulation-enters-force-2024-12-10_en>.

Labelling remains a fundamental instrument for communicating risks to consumers and thereby addressing the bioethical concern of informed consent. It functions as a well-established regulatory mechanism to provide essential hazard information to a broad range of stakeholders, including purchasers, workers, downstream users, and the public. Once adequate disclosure is achieved through labelling, these regulations also serve a protective function, limiting the liability exposure of producers and suppliers.

Typically, labels contain critical information about a product's composition, thereby enabling consumers and end-users to make informed decisions and consciously weigh risks against benefits. However, in the case of nanotechnology, the persistent lack of comprehensive scientific data complicates the determination of appropriate and sufficient labelling requirements for products containing nanoscale materials.

3. Producer Liability and the "Development Risk Defense" Clause.

The issue concerns the concept of development risk, which departs from simplified models of product defectiveness and may be understood as a latent defect. It refers to a defect whose identification depends on circumstances and facts that were unforeseeable at the time the product was placed on the market.

The central issue lies in determining the conditions for exemption from liability, which requires evaluating whether the producer discharged a duty of investigation and testing prior to commercialization. The precautionary principle introduces a new dimension of liability, incorporating anticipatory and preventive elements in light of an uncertain and potentially harmful future. The focus thereby shifts from repairing actual damage to addressing risk itself, to the extent that even the mere creation of risk may constitute a sufficient basis for compensation, implying a conscious acceptance of risk.

This gives rise to a significant concern: the producer – who frequently acts both as the primary researcher and financial sponsor of scientific and technical research – may find themselves in the paradoxical position of being both actor and judge of their own responsibility.

The development risk clause (DRC), already included in Directive 85/374/EEC, provides for an exemption from liability where the producer could not have known of the defect at the time the product was placed on the market, given the state of scientific and technical knowledge then available.

The case law of the Court of Justice of the European Union has reinforced the importance of development risk. In Case C-300/95, the Court held that, to invoke the exemption under Article 7(e) of the Directive, the producer must prove that, at the time the product was placed on the market, the state of scientific and technical knowledge – objectively assessed at the highest available level – did not allow the defect to be detected. The Court further clarified that the exemption is not based on the actual knowledge of the specific producer but on the objective state of knowledge presumed to be accessible at that time.

The legal significance of development risk lies in the need to strike a balance: on the one hand, fostering and encouraging corporate innovation; on the other, meeting the legitimate expectations of consumers, particularly in relation to product safety. [16]

Development risk thus derives from a defect inherent in the product, rendering it dangerous from the moment of its commercialization – a defect that was neither visible nor detectable given the state of scientific or technical knowledge available at the time.

The notion of objective knowledge of the defect is of central importance, as it provides the benchmark for assessing the producer's conduct. This evaluation must consider the scientific and technical knowledge available at the relevant time, and the fact that, once doubts were raised concerning a potential danger, the producer may have had the opportunity to contain or mitigate the progression of future harm.

It is evident that the development risk exemption primarily seeks to balance the need to promote and incentivize innovation with the legitimate expectations of consumers regarding product safety. [17]

Development risk stems from a defect inherent in the product, which must be regarded as dangerous at the time of its placement on the market, even if such danger could not have been detected on the basis of the scientific and technical knowledge then available. Precisely because of this intrinsic hazardous character, the producer, consistent with the precautionary principle, has a duty to adopt appropriate safety measures.

In this context, the notion of objective knowledge at the time of market placement is critical. It serves as the benchmark for determining whether the producer acted negligently by failing to identify scientific or technical information that could have revealed the defect, and whether precautionary measures should have been adopted to prevent or mitigate the resulting harm.

Accordingly, the availability and accessibility of objective knowledge at the relevant time become decisive factors in determining whether the producer fulfilled their duty of care and may legitimately invoke the development risk exemption as a defence against liability.

The new proposal for a Directive on liability for defective products (Product Liability Directive – PLD) [18] introduces a significant reform of the so-called "development risk defence," thereby reshaping the traditional balance between producer protection and consumer and end-user safeguards.

Article 10, entitled "Exemption from liability", reiterates the defence whereby a producer may be exempted from liability if he proves that "the objective state of scientific and technical knowledge at the time when the product was placed on the market, put into service, or within the

[16] G Capilli, 'Principe de précaution et responsabilité civil', *Le Consommateur*, vol 57, (Bruylant Paris 2007) 395–406.

[17] For a comparative analysis on the development risk defence: L Di Donna, 'I regimi di responsabilità applicabili ai danni derivanti dai prodotti farmaceutici – Liability regimes applicable to damages arising from pharmaceutical products' (2024) 1–2 Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario) 117.

[18] G Afferni, 'La nuova direttiva sulla responsabilità per danno da prodotti difettosi: una analisi economica' (2025) 2 Responsabilità Civile e Previdenza 351; A Cioni, 'Nuovi pregi e vecchi difetti della proposta di direttiva sulla responsabilità da prodotto difettoso, con particolare riferimento all'onere della prova' (2023) 2 Responsabilità Civile e Previdenza 656.

manufacturer's control was not such that the defect could be discovered" (Art. 10(e)). This provision echoes the classical formulation of the development risk clause, originally codified in Directive 85/374/EEC, but is reinterpreted in light of the contemporary technological landscape, including digital products and artificial intelligence systems.

The most remarkable innovation, however, lies in Article 18, devoted explicitly to "Derogation from development risk defence", which empowers Member States to restrict or even abolish the availability of such an exemption. This legislative choice signals a profound shift of perspective: no longer a generalised immunity for producers in the name of technological progress, but rather an exceptional and derogable defence, to be balanced against the overriding requirement of ensuring a high level of protection for injured parties (Art. 18).

This orientation is further supported by the recitals. Recital 34 provides that national courts should presume either the defectiveness of a product, the causal link between defectiveness and damage, or both, where, notwithstanding the defendant's duty of disclosure, it would be excessively difficult for the claimant to discharge the burden of proof due to the scientific or technical complexity of the case. To impose strict proof in such circumstances would undermine the very effectiveness of the right to compensation. Consequently, since manufacturers possess expert knowledge and privileged access to information, it falls upon them to rebut the presumption (Recital 34).

At the same time, Recital 39 reiterates the need for a fair allocation of risks, clarifying that the development risk defence applies only where the producer can demonstrate that the state of scientific and technical knowledge – assessed with reference to the most advanced level of objective knowledge accessible, rather than the actual knowledge of the producer – was such that the defect could not have been discovered while the product was under the producer's control (Recital 39).

In conclusion, the new PLD reshapes and circumscribes the scope of the development risk defence, transforming it into a limited and potentially inapplicable clause, in order to reinforce the position of consumers and end-users.[19] This normative choice is consistent with the overarching objective of European product liability law: to provide more effective protection to victims of defective products in contexts of heightened technological complexity, including innovative medical devices, artificial intelligence systems, and connected digital products.

[19] G Afferni, 'La nuova direttiva sulla responsabilità per danno da prodotti difettosi: una analisi economica': "*Come regola generale sembra quindi corretto escludere che il fabbricante possa essere tenuto oggettivamente responsabile anche per i difetti del prodotto che non potevano essere considerati tali in base alle conoscenze scientifiche e tecniche del tempo in cui il prodotto è stato messo in circolazione. Ciò non esclude ovviamente l'operare della responsabilità per colpa. In particolare, il fabbricante può essere tenuto responsabile per il danno causato qualora il consumatore dimostri, eventualmente anche solo per presunzioni, alla luce di tutte le circostanze del caso (tipo di prodotto, dimensioni del fabbricante, tipo di informazioni disponibili, ecc.), che il fabbricante ha colpevolmente omesso di svolgere attività di ricerca e sviluppo al fine di far avanzare, avendone le possibilità, lo stato delle conoscenze scientifiche o tecniche del tempo*".

4. Burden of Proof (New Directive (EU) 2024/2853).

Another significant aspect of analysis in this context concerns the allocation of the burden of proof in product liability cases. Consumers are often placed in a position of structural disadvantage: they generally lack the technical expertise necessary to establish the hazardous nature of a product and are simultaneously deprived of the informational resources that remain predominantly under the control of producers. Such asymmetries create a fundamental imbalance in the evidentiary process, which has historically hindered the effective exercise of consumer rights.

It is precisely against this backdrop that the new PLD represents a notable advancement in consumer protection. Article 10, in this context, introduces an innovative approach specifically designed to mitigate disparities between claimants and producers in technologically complex domains. By adapting evidentiary rules to the realities of contemporary technological markets, the Directive seeks to reconcile the promotion of innovation with the protection of those potentially harmed by emerging products. [20]

The practical implications of Article 10 can be illustrated through a hypothetical scenario. Consider a consumer, Mrs X, who purchases and regularly uses an anti-aging cosmetic cream produced by the Y company, which contains zinc oxide nanoparticles coated with novel polymers. After several months of application, she develops chronic dermatitis with permanent skin lesions and initiates proceedings under the product liability regime. Under the traditional legal framework, such a claim would likely fail: the requirement to establish with scientific certainty a causal link between exposure to nanoparticles and the resulting medical condition imposes an evidentiary burden that is, in practice, insurmountable for the consumer, thereby limiting access to justice.

In response to such challenges, Article 10 functions as a mechanism for evidentiary rebalancing. Paragraph 1 reiterates the general principle that the claimant bears the burden of proving the defectiveness of the product, the harm suffered, and the causal nexus between the two. This principle, however, is substantially qualified by the presumptions introduced in the subsequent paragraphs. Paragraph 2 establishes a presumption of defectiveness where the product fails to comply with mandatory safety requirements. In the hypothetical scenario, the omission of the mandatory label indication regarding the presence of nanoparticles, in violation of EU cosmetics regulations, triggers the presumption of defectiveness. Paragraph 3 further provides for a presumption of causation where the type of harm suffered is typically consistent with the alleged defect: chronic dermatitis constitutes a harm inherently compatible with exposure to undisclosed chemical or nano-ingredients.

The most innovative element is found in paragraph 4, which recognises that, in cases characterised by significant scientific or technical complexity, it is

[20] Moritz Becker, Anita Bell, Hannah Meyer, 'Product Risks Today: How the new Product Liability Directive facilitates private enforcement' (*Freshfields*, 1 April 2025) <https://riskandcompliance.freshfields.com/post/102k71h/product-risks-today-how-the-new-product-liability-directive-facilitates-private>.

unreasonable to expect the consumer to discharge an excessive evidentiary burden. Where the claimant adduces sufficient evidence to render defectiveness or causation plausible, the court may presume their existence. This provision is particularly well-suited to nanotechnological products, where scientific knowledge remains in development and critical information continues to be largely controlled by producers. Paragraph 5 safeguards the producer's right to rebut such presumptions; yet the underlying principle is unambiguous: the burden of scientific uncertainty can no longer rest exclusively on the consumer.

Viewed in light of the hypothetical scenario, Article 10 underscores a considerable enhancement of consumer protection under the new regime. Whereas under the previous framework the absence of conclusive scientific evidence would have almost certainly precluded redress, the revised provisions enable the activation of legal presumptions, thereby facilitating consumer access to justice. The Directive effectively redistributes the risks associated with evidentiary uncertainty, requiring producers to provide convincing counter-evidence in order to rebut the presumptions.

In conclusion, Article 10 of the Directive constitutes a decisive step forward in the protection of consumers exposed to risks arising from emerging technologies, such as nanomaterials. It signifies a paradigm shift: scientific uncertainty, which previously served to deny redress, is now employed as a criterion to strengthen consumer protection. By aligning evidentiary rules with the realities of technologically sophisticated markets, the Directive ensures that the advancement of innovation does not occur at the expense of justice for individuals harmed by unsafe products.

5. Conclusion.

The legal treatment of nanotechnologies within the framework of product liability requires a dual perspective: one grounded in regulatory precaution and another rooted in civil liability doctrines. While regulation provides ex ante safeguards by restricting or banning certain nanomaterials, civil liability continues to operate ex post, ensuring redress for harms not prevented by regulatory standards. The dynamic interplay between these two dimensions is particularly evident in light of the most recent amendments introduced by Commission Regulation (EU) 2024/858 to Regulation (EC) No 1223/2009 on cosmetic products.[21]

The regulatory prohibition of specific nanomaterials – such as styrene/acrylates copolymer (nano) and sodium styrene/acrylates copolymer (nano) – and the restrictions imposed on colloidal silver (nano) and hydroxyapatite (nano) are not predicated upon conclusive causal evidence of

[21] European Commission, Official Journal L_202400858 <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:L_202400858>, accessed 6 October 2025; Scientific Committee on Consumer Safety (SCCS), Opinion on Titanium Dioxide (Nano Form), SCCS/1617/20 (2022) <https://health.ec.europa.eu/system/files/2022-08/sccs_o_239.pdf>, accessed 6 October 2025; Normachem, Nuove restrizioni dell'uso di nanomateriali: la cosmetica perde 9 ingredienti (2024) <https://www.normachem.com/it/normachem-informa/nuove-restrizioni-delluso-di-nanomateriali-la-cosmetica-perde-9-ingredienti> accessed 6 October 2025.

harm. Rather, they are grounded in the precautionary principle, reflecting the recognition that preliminary toxicological data on genotoxicity, cytotoxicity, organ toxicity, and nanoparticle bioaccumulation are sufficient to justify preventive measures. This regulatory choice carries significant implications for the assessment of liability in civil law.

First, the definition of "defect" under the EU Product Liability Directive and corresponding national regimes must be read in light of evolving regulatory standards. A product incorporating a nanomaterial that is later banned or restricted by regulation may retrospectively be considered "defective," even if it complied with standards at the time of placing on the market, insofar as consumer expectations of safety are objectively shaped by the regulatory context. Second, the duty to warn – long recognised as a cornerstone of product safety law – acquires heightened relevance in the field of nanotechnologies. The persistent scarcity of toxicological data implies that producers have a positive obligation to continuously monitor emerging scientific knowledge, to update risk assessments, and to provide transparent warnings to consumers and intermediaries. Omission or insufficiency in this regard may constitute a basis for liability, independent of regulatory compliance.

Third, the burden of proof in toxic torts – traditionally placed on the injured party – becomes problematic in the context of nanomaterials, where causation is difficult to establish due to the novelty and complexity of exposure pathways. The application of the precautionary principle at the regulatory level strengthens the argument for a more flexible evidentiary approach in civil proceedings, whether through presumptions of causation, a reversal of the burden of proof, or an expansive interpretation of strict liability. Such adaptations would better reflect the structural epistemic uncertainty inherent to nanotechnologies, while aligning liability doctrines with the preventive rationale underlying EU regulatory action.

In conclusion, the regulation of cosmetic nanomaterials under Regulation (EU) 2024/858 provides a paradigmatic example of how precaution operates as a bridge between product safety regulation and civil liability. It demonstrates that, in a field marked by continuous scientific evolution, liability doctrines must not merely react to proven harm, but must integrate precaution as a guiding interpretative principle. This evolution ensures that producers remain vigilant and proactive in addressing potential risks, thereby aligning civil liability with the broader constitutional objective of safeguarding health and consumer protection in the era of nanotechnology.

Ciocia MA, 'Il Greenwashing: asimmetrie di mercato e interventi normativi nell'Unione Europea' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252MAC

EJPLT
ISSN 2704-8012



Il Greenwashing: asimmetrie di mercato e interventi normativi nell'Unione Europea

Greenwashing: market asymmetries and regulatory measures in the European Union

MARIA ANTONIA CIOCIA
Professore Ordinario di Diritto Privato
Università della Campania Luigi Vanvitelli

Abstract

Il greenwashing è una fattispecie di marketing ingannevole caratterizzata dal fatto che le aziende promuovono un'immagine ecosostenibile allo scopo di nascondere un impatto ambientale negativo e migliorare la propria reputazione sul mercato. Avverso tale pratica il legislatore comunitario ha adottato una strategia legislativa capillare intervenendo nella fase genetica della formazione del consenso del consumatore che deve sempre essere pienamente informato e non fuorviato da pratiche commerciali ingannevoli. Una strategia coerente a livello europeo è in atto, un ruolo fondamentale per il successo della pianificazione comunitaria sarà rappresentato dal fedele recepimento della direttiva in tutti gli Stati membri e dalla consapevolezza negli atti di vendita e di acquisto di produttori e consumatori.

Greenwashing is a form of misleading marketing characterized by companies promoting an eco-sustainable image with the aim of concealing a negative environmental impact and improving their market reputation. The European Union legislator has adopted a comprehensive legislative strategy to combat this practice, intervening at the early stages of consumer consent formation. Consumers must always be fully informed and not misled by deceptive commercial practices. A coherent European strategy is in place; faithful transposition of the directive in all Member States and awareness in sales and purchasing practices by producers and consumers will play a key role in the success of this EU strategy.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: sostenibilità; consumatore; informazioni; produttore; greenwashing

Summary: 1. Introduzione. – 2. La tassonomia nei mercati finanziari. – 3. Il contrasto all'"ingannevolezza" nella tutela del consumatore. – 4. Il ruolo dell'autodisciplina pubblicitaria nell'ordinamento italiano. – 5. La direttiva 2024/825/UE e la tutela del consumatore. – 6. Il greenwashing e la configurabilità del danno alla sostenibilità. – 7. Responsabilità negoziale e greenwashing. – 8. Altre fattispecie sanzionatorie per arginare il greenwashing. – 9. La falsa dichiarazione oltre la sostenibilità nei rapporti con la pubblica amministrazione. – 10. Provvedimenti giurisdizionali a tutela del mercato e del consumatore. – 11. Il contrasto all'obsolescenza programmata. – 12. Conclusioni.

1. Introduzione.

Nel contesto di un mercato fortemente competitivo, il consumatore non valuta più solo il bene materiale in sé (il prodotto di base) per l'uso o l'interesse che è destinato a soddisfare, ma è attratto da una serie di attributi e fattori differenziali. Diviene rilevante per il produttore evidenziare i pregi del prodotto immesso sul mercato, in modo che sia immediato e palese il vantaggio competitivo rispetto ad altri beni di medesimo genere. In questi termini, l'accelerazione del fenomeno produttivo, la funzionalità e l'efficientismo dell'autonomia privata hanno rafforzato il dogma dell'apparenza idoneo a veicolare le qualità vantate dal prodotto che, talvolta però, possono non essere rispondenti alle caratteristiche promesse[1]. Recentemente, la competizione nel mercato viene a svolgersi sul piano della tecnologia green adottata dal produttore, esaltata in quanto improntata a canoni di "sostenibilità ambientale"[2]. Dal quadro delineato risulta evidente che l'aspetto più rilevante

[1] A. Bassi, M. Lamandini, A. Troisi, F. Vella, *Greenwashing e tutela del consumatore per un'economia sostenibile*, in *Quaderni giuridici Consob*, 33, Roma, 2025, 30, ove si fa riferimento alla curiosa fortuna nel lessico corrente dell'espressione "greenwashing", a designare, in via di prima approssimazione, tutte le possibili manifestazioni di comunicazione dell'impresa che vantino o comunque presentino di essa una coerenza con gli obiettivi di sostenibilità che essa concretamente non ha, o non ha nei termini rivendicati. S. Lanni, G. Magri, *Mercato digitale e nuovi paradigmi della tutela del consumatore in Brasile e Germania,* in *Annuario di diritto comparato*, 2017, 917 ss.

[2] Cfr. Sul concetto di sostenibilità, agli albori F. Lucarelli, *Il Sud ed il caso Brasile. Il monitoraggio ambientale*, in *Diritto all'ambiente Procedure d'impatto, Earth summit Rio de Janeiro Giugno '92*, Napoli, 1992, 119-140; P. Perlingieri, *I diritti umani come base dello sviluppo sostenibile. Aspetti giuridici e sociologici,* in Id., *La persona e i suoi diritti. Problemi di diritto civile*, Napoli, 2005, 73 ss.; M. Pennasilico, *Sostenibilità ambientale e riconcettualizzazione delle categorie civilistiche*, in Aa.Vv., *Manuale di diritto civile dell'ambiente*, a cura di M. Pennasilico, Napoli, 2014, 34 ss. Per una analisi informata alla bibliografia italiana sulla sostenibilità cfr. D. Imbruglia, *Verso un diritto del consumo sostenibile*, in *Iniziativa economica privata e mercato unico sostenibile*, a cura di C. Capaldo, Roma, 2023, 113 ss.; C. Mignone, *Diritti e sostenibilità. Una ricostruzione per immagini,* in *Actualidad Jurídica Iberoamericana*, 2021, 211 e in particolare nt 9. Sulle origini del principio dello sviluppo sostenibile, si vedano F. Fracchia, S. Vernile, *Lo sviluppo sostenibile oltre il diritto ambientale,* in *Le Regioni*, 2022, 15 ss. Sulla sostenibilità quale limite allo sviluppo indiscriminato e abusivo si veda M. Pennasilico, *Sviluppo sostenibile e "contratto ecologico": un altro modo di soddisfare i bisogni*, in *Rass. dir. civ.*, 2016, 1291 ss.; A. Buonfante, A. Uricchio, *Trattato breve di diritto dello sviluppo sostenibile,* 7, Milano, 2023, 29-37, in particolare, sul cambio di paradigma nel segno della solidarietà globale, dell'etica intergenerazionale e della responsabilità condivisa e sugli effetti della costituzionalizzazione della tutela ambientale. M. Nocenzi, *Sostenibilità e sviluppo sostenibile. Una lettura transdisciplinare,* 2025, 1-258; M. Pennasilico, *Emergenza e*

della tutela del consumatore diviene la rispondenza del prodotto alle qualità promesse dal produttore. A livello unionale il Parlamento Europeo e il Consiglio d'Europa sono intervenuti con l'emanazione di vari atti, nel loro complesso complementari, ma tutti coesi alla realizzazione di un mercato sostenibile dal punto di vista ambientale. Il nemico da sconfiggere è la falsa sostenibilità sintetizzabile nel termine "greenwashing"[3].

2. La tassonomia nei mercati finanziari.

Un primo intervento per il contrasto alla prassi del greenwashing, si è svolto sul piano classificatorio, nel senso di individuare le attività economiche che possono ritenersi "sostenibili". Il Parlamento europeo[4] con il regolamento sulla

ambiente all'epoca pandemica. Verso un diritto dello "sviluppo umano ed ecologico", in *Giustizia civile*, 2021, 495; M.A. CIOCIA, *La sostenibilità ambientale in epoca pandemica,* Milano, 2020, 3 e ss.; S. COSIMATO, *Sviluppo sostenibile e imprenditorialità. Competitività e innovazione nelle PMI,* Napoli, 2015, 13 ss.; M. STRADA, L.P. VECCHIO, *Sostenibilità e sviluppo sostenibile: analogie e differenze. Uno studio su rappresentazioni e valori legati ai due costrutti*. Intervento presentato a: Congresso Nazione di Psicologia per le Organizzazioni, Palermo, 2015, in cui gli autori rilevano come benché ormai accettati e "dati per scontato", tali termini si caratterizzano per ambiguità, confusione, vaghezza e contraddittorietà nell'utilizzo. S. TOMMASI, *Dalla sostenibilità declamata alla sostenibilità effettiva nella direttiva (EU) 2024/825: l'empowering consumers for the green transition*, in *Rivista di diritto dell'economia, dei trasporti e dell'ambiente*, vol. XXII, 2024, 727-744. Per una visione anche transeuropea della sostenibilità cfr. D. B. AKKERMANS, G.VAN DIJCK (a cura di), *Sustainability and Private Law*, Netherlands, 2020. Sulla pluralità di significati dello sviluppo sostenibile, si vedano H.M. FARLEY, L.A. SMITH, *Sustainability If It's Everything, Is It Nothing*?, London, 2020; F. EKARDT, *Sustainability. Transformation, Governance, Ethics, Law, Cham*, 2020; J. CARADONNA, *Sustainability. A history,* Oxford, 2016; V. MAUERHOFER, *The Role of Law in Governing Sustainability*, London, 2021.

[3] Greenwashing, Il termine greenwashing nasce dalla fusione di green (verde, colore dell'ecologismo) e washing dal verbo inglese to wash (lavare). In dottrina, *ex multis*, C. COSENTINO, *"Environmental claims": quando la disinformazione "si veste di verde"*, in *Comparazione e diritto civile,* 2023, 79 ss.; A. LEONE, *Advertising e tutela del consumatore verde*, in *Dir. ind.*, 2021, 73 ss.; M. LIBERTINI, *La comunicazione pubblicitaria e l'azione delle imprese per il miglioramento ambientale*, in *Giur. comm.*, 2012, 331; R. KORN, *Tutela dell'ambiente, consumatori e responsabilità sociale d'impresa: i nuovi strumenti della sostenibilità aziendale,* in *Contr. impr. eur.*, 2012, 671; A. TROISI, *La comunicazione ambientale: il greenwashing dietro la sostenibilità*, in *An. giur. ec.,* 2022, 353 ss.; F. BERTELLI, *I green claims tra diritti del consumatore e tutela della concorrenza,* in *Contr. e impr.*, 2021, 286 ss., M. TAVELLA, *Comunicazione, marketing e sostenibilità ambientale*, Torino, 2012, *passim;* R. LUCIANI, M. D'AMICO, L. ANDRIOLA, *La comunicazione ambientale e sociale d'impresa: stato dell'arte e nuovi orientamenti,* in *Amb.,* 2005, 757; S. CARMIGNANI, *L'informazione ai tempi della sostenibilità,* in *Riv. dir. alimentare*, 2024, 27 ss.; F. IRALDO, M. MELIS, *Come evitare il greenwashing comunicando il valore della sostenibilità*, Milano, 2012, *passim;* in termini aziendali: "tendenza da parte delle imprese a fornire informazioni non sempre corrette in merito all'effettivo impatto ambientale o sociale delle proprie attività, al fine di ingenerare un'erronea rappresentazione nelle menti dei consumatori; questo fenomeno è notoriamente identificato con il termine "Greenwashing" così A. DAVOLA, *Informativa in materia di prodotti finanziari sostenibili, tutela dell'investitore e contrasto al greenwashing: le criticità dell'assetto europeo tra norme primarie e disciplina di dettaglio*, in *Riv. di dir. Banc.*, 2022, 3, I, 514; G. SPEDICATO, *Il corporate greenwashing come pratica commerciale sleale,* in *Quaderni di giurisprudenza commerciale*, 467, Milano, 2025, 297, ove viene evidenziato come il Greenwashing non sia definito nel nostro ordinamento, allo stato solo la Regione Puglia nella legge regionale del 12 agosto 2022 n. 18 , all'art. 2 prevede la costituzione di un Albo regionale delle società benefit pugliesi e menziona il greenwashing come rischio per i consumatori e le imprese che la costituzione del suddetto albo regionale dovrebbe contribuire a prevenire tale prassi.

[4] Tra le iniziative intraprese si trova il regolamento sui benchmark (Regolamento 2019/2089/UE, che modifica il precedente Regolamento 2016/1011/UE), il quale introduce indici di riferimento di transizione climatica e allineati all'Accordo di Parigi. stabilisce un quadro normativo europeo per garantire l'accuratezza e l'integrità degli indici di riferimento. Aggiornato per contrastare il greenwashing**,** impone standard di trasparenza severi, richiedendo agli amministratori di divulgare come i fattori ESG (Ambientali, Sociali, di Governance) influenzano la metodologia di calcolo di ciascun benchmark, per approfondimento cfr. A. DAVOLA, *Informativa di sostenibilità, tutela dell'investitore e contrasto al greenwashing. Le criticità dell'assetto europeo tra norme primarie e disciplina di dettaglio*, in *Dir. Bancario*. Si veda, in tal senso, l'indagine Condotta da IBM, *Meet the 2020 consumers driving change. Why brands must deliver on omnipresence, agility, and*

tassonomia [5], ha inteso definire univocamente, nel contesto dei mercati finanziari, il concetto di «attività economica sostenibile dal punto di vista ambientale [6]», onde rendere chiaro agli investitori il tasso di sostenibilità dell'azienda alla quale destinare i propri flussi di capitali d'investimento, riferimento rilevante per gestori finanziari e agenzie di rating[7]. Il Regolamento, definisce ecosostenibile un'attività economica che contribuisce in maniera sostanziale a uno o più obiettivi ambientali dell'Agenda 2030, senza sacrificarne alcuno e senza violare i diritti umani. L'ottica del regolamento è evidentemente parziale perché il perseguimento di un obiettivo tra quelli dell'Agenda 2030 non dà garanzia di assolutezza in ordine alla sostenibilità [8] ben potendo cumularsi con ulteriori finalità non allineate al green pledge. Sono annoverabili altre iniziative dell'Unione Europea, incluse nella nuova Agenda dei consumatori (2020-2025), quali, nello specifico, il Green Consumption Pledge (2021) - impegno per consumi sostenibili, finalizzato a rafforzare il ruolo dei consumatori nella transizione verde, cui si accompagna la proposta legislativa europea sulla dimostrazione della veridicità delle affermazioni ecologiche.[9] Il Regolamento (UE) n. 2019/2088, Sustainable Finance Disclosure Regulation

sustainability, 2020. Consultabile online: https://www.ibm.com/downloads/cas/EXK4XKX8; cfr. altresì R. ROSMARIN, *Sustainability sells: Why consumers and clothing brands alike are turning to sustainability as a guiding light,* 2020. Consultabile online: www.businessinsider.com.

[5] Regolamento 2020/852/UE del Parlamento europeo e del Consiglio del 18 giugno 2020 relativo all'istituzione di un quadro che favorisce gli investimenti sostenibili e modifica il Regolamento 2019/2088/UE. Cfr. *Platform on Sustainable Finance, Draft Report on Social Taxonomy,* luglio 2021*; Platform on Sustainable Finance, Report on Taxonomy extension options linked to environmental objectives,* luglio 2021*; Platform on Sustainable Finance, Transition Finance Report,* marzo 2021. Consultabile online: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlkfl8byxup5?ctx=vg9pjk198axu&start_tab0=40. V. anche A. MOONEY, *Greenwashing in finance: Europe's push to police ESG investing*, 2021. Consultabile online: https://www.ft.com/content/74888921-368d-42e1-91cd- c3c8ce64a05e.

[6] M. TOMMASO, *Strategia europea sulla finanza sostenibile informazione societaria e possibili riflessi sulla gestione della società,* in *Giur. comm.* 2023, I, 607; M. COSSU, *Sostenibilità e mercati: la sostenibilità ambientale dell'impresa dai mercati reali ai mercati finanziari*, in *BBTC*, 2023, 558; C. AMATUCCI, *Responsabilità sociale dell'impresa e nuovi obblighi degli amministratori. La giusta via di alcuni legislatori*, in *Giur. comm.*, 2022, I, 612; G. RACUGNO, D. SCANU*, Il dovere di diligenza delle imprese ai fini della sostenibilità: verso il Green deal europeo,* in *Giur. comm.*, 2022, I, 726; AA.VV., *Sostenibilità Profili giuridici, economici e manageriali delle PMI italiane*, a cura di F. MASSA, Torino, 2019; AA.VV., *L'impresa sostenibile Alla prova del dialogo dei saperi,* a cura di D. CATERINO, I. INGRAVALLO, Lecce, 2020; M. MAUGERI, *Informazione non finanziaria e interesse sociale,* in *Riv. so*c., 2019, 992; P. DE GIOIA CARABELLESE, *Corporate Social Responsibility e Common Law,* in *Giur. Comm.*, I, 2019, 1041; C. ANGELICI, *Divagazioni sulla "responsabilità sociale" d'impresa,* in *Riv. soc.*, 2018, 3.

[7] Il rating esprime un giudizio che certifica la solidità e l'affidabilità di un emittente, di un titolo, di un fondo. Può essere utile agli stakeholders per valutare il grado di sostenibilità di un'impresa. Cfr. M. MEGGIOLARO, «*Rate the raters»: gli operatori del rating di sostenibilità e i loro metodi a confronto*, in *Creare valore a lungo termine,* a cura di D. DAL MASO, G. FIORENTINI, Milano, 2013, 113. Sul tema anche M. GARANTINI, M. SIRI, *Information Intermediaries and Sustainability ESG ratings and benchmarks in the European Union, ECMI Working Paper*, 15, 2022; M. SIRI, S. ZHU, *L'integrazione della sostenibilità nel sistema europeo di protezione degli investitori,* in *Banca impr. soc.,* 2020, 3; E. BELISARIO, *Rischi di sostenibilità e obblighi di discolsure: il D. Lgs. n. 254/16 di attuazione della dir. 2014/95/UE*, in *Nuove leggi civ. comm.,* 2017, 19; V. BUONOCORE, *Etica degli affari, impresa etica e impresa socialmente responsabile*, in *La responsabilità sociale dell'impresa,* a cura di G. CONTE, Roma-Bari, 2008, 46; S. BRUNO, *Dichiarazione "non finanziaria" e obbligo degli amministratori,* in *Riv. soc.,* 2018, 974.

[8] S.FIANDRINO, R. RASCHILLÀ, *L'evoluzione del quadro normativo sovranazionale e nazionale in materia di sostenibilità, Sostenibilità e Fattori ESG*, Torino, 2025, 15-51.

[9] In questa strategia si inserisce anche l'introduzione dell'obbligo di dotare i prodotti alimentari di etichette nutrizionali armonizzate tra gli Stati membri, nonché dell'obbligo di etichetta energetica UE per gli elettrodomestici, al fine di permettere ai consumatori di conoscere l'efficienza energetica di taluni prodotti e di acquistarli nella consapevolezza di reali risparmi. Sul tema cfr. M. GIOIA, *L'etichettatura dei prodotti alimentari dopo il Reg. (CE) n. 178/2002: nuove etichette e educazione del consumatore*, in *Rivista di diritto alimentare*, 2023, 1, 20.

«Regolamento SFDR» o anche solo «SFDR»[10], relativo all'informativa sulla sostenibilità nel settore dei servizi finanziari, prevede poi un insieme di rilevanti obblighi di *disclosure* in tema sostenibilità[11]. Le scelte di investimento sostenibili dipendono, innanzitutto, dalla possibilità di disporre di informazioni[12]. Con il regolamento SFDR l'obbligo informativo è posto a carico di determinati soggetti, i partecipanti ai mercati e consulenti finanziari, con la previsione di fornire informative sull'integrazione dei rischi di sostenibilità e sulla considerazione, nelle politiche di investimento, degli eventuali effetti negativi sulla sostenibilità[13].

[10] Regolamento (UE) 2019/2088 del Parlamento europeo e del Consiglio del 27 novembre 2019, relativo all'informativa sulla sostenibilità nel settore dei servizi finanziari. Cfr. D. DAL MASO (a cura di), *Investire nella sostenibilità. Diffusione e prospettive SRI nel private banking*, *cit.*, 35; Cfr. *Comunicare la sostenibilità il punto di vista degli emittenti* di P. GIANGUALANO P. SCHWIZER, *Investire nella sostenibilità. Diffusione e prospettive SRI nel private banking*, AIPB- Associazione Italiana *Private Banking*, Milano, 2019, 81.

[11] Il regolamento, come rilevato dal Considerando 11, integra gli obblighi informativi previsti dal corpus normativo costituito dalle direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2014/65/UE, (UE) 2016/97, (UE) 2016/2341, nonché dai regolamenti (UE) n. 345/2013, (UE) n. 346/2013, (UE) 2015/760 e (UE) 2019/1238. Per aspetti civilistici nel nostro ordinamento cfr. G. ALPA, *Responsabilità degli amministratori di società e principio di «sostenibilità»*, in *Contr. Impr.*, 2021, 3, 721 e ss., F. CAPRIGLIONE, *Il sistema finanziario verso una transizione sostenibile*, in *Riv. trim. dir. econ.*, 2021, 1, I, 241 ss.; di recente, altresì F. RIGANTI, *Regolazione del mercato e "fine di lucro". Spunti per una ricerca attualizzata in tema di sostenibilità*, 4 maggio 2022, in *Dirittobancario.it.*; D. DAL MASO (a cura di), *Investire nella sostenibilità. Diffusione e prospettive SRI nel private banking*, *cit.*, 35. Cfr. *Comunicare la sostenibilità il punto di vista degli emittenti* di P. GIANGUALANO, P. SCHWIZER, *op. cit.*.

[12] V. CALANDRA BUONAURA, *Responsabilità sociale dell'impresa e doveri degli amministratori*, in *Giur. comm.,* 2011, I, 526; R. COSTI*, La responsabilità sociale dell'impresa e il diritto azionario italiano*, in AA.VV*., La responsabilità dell'impresa. Per i trent'anni di Giurisprudenza Commerciale,* Milano, 2006, 83; F. FRACCHIA, *Sviluppo sostenibile e diritti delle generazioni future,* in *Rivista Quadrimestrale di Diritto dell'Ambiente*, 2010, 15.

[13] D. BUSCH, *Sustainability Disclosure in the EU Financial Sector, 6 aprile 2021*; *European Banking Institute Working Paper Series*, 2021, n. 70; M. STELLA RICHTER, *Long-termism*, in *Riv. Soc.*, 2021, 16; P. BENAZZO, *Organizzazione e gestione dell'«impresa complessa»: compliance, adeguatezza ed efficienza. Ex pluribus unum*, in *Riv. soc.*, 2020, 1197; E. GIOVANNINI, *Non c'è un futuro sostenibile senza l'impegno delle imprese ad attuare l'Agenda 2030*, in *Quaderni di approfondimento 2023, ESG e SRI, le politiche di investimento sostenibile degli investitori istituzionali italiani. Quinta indagine sulle strategie di sostenibilità e integrazione dei criteri ESG nei portafogli dei principali investitori istituzionali italiani*, a cura del Centro Studi e Ricerche Itinerari Previdenziali, 2023, 13-16.

3. Il contrasto all'"ingannevolezza" nella tutela del consumatore.

La direttiva Omnibus[14] delinea l'ambito della pratica commerciale sleale e distingue l'azione ingannevole [15] dall'omissione ingannevole [16] entrambe caratterizzate da informazioni non veritiere che inducono falsamente la decisione di acquisto[17]. La direttiva introduce sanzioni severe[18], viene recepita in Italia con il d. lgs. n. 26/2023, per intervenire nei rapporti tra professionista e consumatore[19] nei negozi online o anche fisici e impegnare i venditori alla

[14] Direttiva (UE) 2019/2161 del 27 novembre 2019, entrata in vigore con il recepimento in Italia attraverso il D. lgs. 26 del 2023, del 18 marzo 2023 pubblicato in Gazzetta Ufficiale ad aprile 2023 finalizzata alla tutela del consumatore nell'ambito del "*New Deal for Consume*rs" attraverso la regolamentazione dell'impianto normativo in seguito all'evoluzione digitale dei nuovi mercati, per una tutela dei consumatori dotata di un maggior grado di effettività. Per approfondimento dottrinario G. VERSACI, *Le tutele a favore del consumatore digitale nella "Direttiva Omnibus"*, in *Persone e Mercato*, 2021, 3, 583-595, che rileva come le modifiche ed integrazioni alle discipline in materia di pratiche commerciali sleali e di obblighi informativi precontrattuali intendono garantire una trasparente dinamica degli atti di consumo nei mercati online. Inoltre, l'autore evidenzia come l'armonizzazione attuata dal legislatore europeo, rischia di risultare nel complesso carente del requisito della coerenza. Anche L. BALESTRA, *Le pratiche commerciali scorrette alla luce della direttiva omnibus* in *Riv. trim. di diritto e procedura civile*, 2025, 51-65. Per la fase antecedente l'emazione della direttiva cfr. L. VIZZONI, *Recensioni non genuine su tripadvisor: quali responsabilità*?, in *R. civ. e prev.*, 2018, 706 ss., spec. 708.

[15] Una pratica commerciale è ingannevole se accompagnata da informazioni false o non veritiere oppure è di per sé idonea ad ingannare il consumatore medio, anche se l'informazione è di per sé corretta, ma intrinsecamente riferita ad elementi che inducono il consumatore ad assumere una decisione di acquisto che altrimenti non avrebbe adottato. Cfr. S. PAGLIANTINI, *Contratti di vendita di beni: armonizzazione massima, parziale e temperata della Dir. UE 2019/771,* in *Giur. it.,* 2020, 217 ss.; G. D'AMICO, S. PAGLIANTINI, *L'armonizzazione degli ordinamenti dell'Unione europea tra principi e regole,* Torino, 2018, *passim.*

[16] Le omissioni ingannevoli si riferiscono ad aspetti del prodotto o del servizio volutamente non dichiarati dal venditore al fine di carpire il consenso all'acquisto del consumatore. F. MASSA, *Omissioni ingannevoli* in *Codice del consumo*, a cura di V. CUFFARO, Milano, 203-215, anche in M. FOTI, *Pratiche commerciali scorrette, dolo determinante e annullamento del contratto, in Rassegna di diritto civile*, 2022, 3, 1126-1156, viene analizzata la pronuncia del Tribunale civile di Salerno n. 259, Sez. II del 20 gennaio 2020, che dispone l'annullamento per dolo di un contratto stipulato 'a valle' di una pratica commerciale scorretta. Il commento si sofferma su questioni interpretative rilevanti, quali i doveri informativi precontrattuali, i rimedi esperibili dal consumatore e il raccordo tra la disciplina codicistica del dolo negoziale e quella speciale in tema di pratiche commerciali scorrette; R. CALVO, *Le azioni e le omissioni ingannevoli*, in *Rass. Dir. Civ.*, 2022, 3, 63 e ss., anche R. CALVO, *Le azioni e le omissioni ingannevoli: il problema della loro sistemazione nel diritto patrimoniale comune*, in *Contr. e impr./Europa*, 2007, I, 78; C. GRANELLI, *Le «pratiche commerciali scorrette» tra imprese e consumatori: l'attuazione della direttiva 2005/29/CE modifica il codice del consumo*, in *Obbl. e contr.*, 2007, 777; P. COTTAFAVI, *Concorrenza sleale, pubblicità e consumatori*, in AA. VV., *Commentario breve alle leggi su Proprietà intellettuale e concorrenza. Appendice di aggiornamento*, a cura di T.M.G. UBERTAZZI, *Art. 20*, Padova, 2008, 97 ss..

[17] Ad esempio, quando il professionista seleziona le recensioni pubblicando solo le positive, commissiona recensioni positive, prassi avverso la quale viene introdotto l'obbligo di chiarire se e quali recensioni provengono dal cliente, in ottica globale cfr. G. MAGRI, *False recensioni di beni o prodotti in internet e responsabilità civile*, in *Revista Brasileira de Direito Civil – RBDCivil | Belo Horizonte*, 2019, Vol. 20, 113-135, in particolare l'articolo approfondisce la questione alla luce della disciplina italiana ed europea in materia di concorrenza sleale e della protezione del consumatore dalle pratiche commerciali sleali, con particolare riferimento alla giurisprudenza dei diversi ordinamenti europei con riferimento alla responsabilità degli ISP.

[18] Decisivo l'impatto sul piano sanzionatorio per cui il mancato rispetto delle norme in relazione alla gravità, entità e durata della violazione comporta l'imposizione di sanzioni che variano da 5 a 10 milioni di euro. Modeste le sanzioni per le errate indicazioni di prezzo che vanno da 516 euro ai 3098 euro. In dottrina cfr. G. AFFERNI, *La responsabilità del venditore per i difetti materiali del bene,* in *Cultura giuridica e rapporti civili*, 2022, Napoli, 340, ove viene rilevata l'imprescrittibilità del diritto del compratore alla restituzione del prezzo e al risarcimento del danno

[19]Non mancano nella fase precedente l'emanazione della direttiva omnibus interventi giurisprudenziali nell'ordinamento nazionale che spostavano il piano dell'intervento sul fronte del diritto penale. In tal senso cfr. Cass. Pen., sez. V, 23.01.2017, n. 8482, in *Guida al diritto* 2017, 16, 98, facendo ricorso alla fattispecie della diffamazione aggravata in questi termini : «L'uso dei social network, e quindi la diffusione di messaggi veicolati a mezzo internet integra un'ipotesi di diffamazione aggravata ai sensi dell'art. 595, comma 3, c.p., poiché trattasi di condotta potenzialmente capace di raggiungere un numero indeterminato o, comunque,

veridicità e alla trasparenza, con il divieto di pubblicare o far pubblicare recensioni false o falsi apprezzamenti [20], punisce altresì pratiche come l'occultamento di informazioni commerciali e prodotti a doppio standard qualitativo [21]. L' l'intervento è parziale [22] e la Commissione europea per implementare la sostenibilità nel mercato e contrastare le diffuse pratiche di greenwashing, emana la Direttiva 2024/825/UE[23] e la proposta contenuta nella COM (2023) [24], "Green claims directive" sui claims ambientali espliciti [25]. Entrambi gli atti sono finalizzati a stigmatizzare le dichiarazioni apparentemente green riportate sulle etichette dei prodotti e nella pubblicità, mediante l'individuazione di canoni chiari e trasparenti da porre alla base dell'eventuale giudizio di "ingannevolezza"[26]. Ruolo centrale viene ricoperto da un organismo indipendente responsabile dell'asseveramento della veridicità delle affermazioni nella fase antecedente la commercializzazione[27]. La stessa Commissione europea il 19 giugno del 2025 ritira la proposta contenuta nella COM (2023) 166, Green claims directive, con l'effetto di attenuare la portata del processo avviato [28]. Interessanti le interpretazioni date al ritiro, che sortiscono l'effetto di evidenziarne i limiti: l'obbligo della verifica preventiva per qualsivoglia dichiarazione, la scarsa coerenza sistemica e l'insufficiente

quantitativamente apprezzabile di persone, qualunque sia la modalità informatica di condivisione e di trasmissione. Del resto, l'art. 595, comma 3, c.p., riferendo la diffamazione aggravata all'uso del mezzo della stampa ovvero disgiuntamente all'uso di ogni altro mezzo di pubblicità, rende evidente come la categoria dei mezzi di pubblicità sia più ampia del concetto di stampa, includendo tutti quei sistemi di comunicazione e, quindi, di diffusione - dal fax ai social media - che, grazie all'evoluzione tecnologica, rendono possibile la trasmissione di dati e notizie a un numero ampio o addirittura indeterminato di soggetti».

[20] Cfr. L. CAROTA, *Diffusione di informazioni in rete e affidamento sulla reputazione digitale dell'impresa,* in *Giur. comm.*, 17, 624 ss.

[21] A. CILENTO, *New deal per i consumatori: risultati all'altezza delle ambizioni?,* in *Contr. impr.*, 2019, 1195 ss, analizza gli aspetti programmatici della direttiva valutando la realizzazione degli effetti sul piano consumeristico; Cfr. anche R. PARDOLESI, R. VAN DEN BERGH, F. WEBER, *Facebook e i peccati da «Konditionenmissbrauch»*, in *Merc. conc. reg.*, 2020, 513 ss. Rilevante applicazione giurisprudenziale.

[22] M. DUROVIC, *Adaptation of consumer law to the digital age: EU Directive 2019/2161 on modernisation and better enforcement of consumer law,* in *Anali Pravnog fakulteta u Beogradu*, 2020, 65. Evidenzia l'attenuazione del processo di armonizzazione a tutela del consumatore.

[23] Anche nota come Direttiva *Empowering Consumers*, approvata a marzo 2024.

[24] Il riferimento alla proposta COM/2023 include i documenti di pianificazione pubblicati dalla Commissione Europea nel 2023 in ambiti strategici quali ambiente, gestione malattie, regolamenti e direttive strategiche.

[25] Proposta, più tecnica e specifica sui metodi di verifica delle dichiarazioni ambientali, è stata sospesa a livello UE nel giugno 2025.In dottrina cfr. B. POZZO, *I green claims, l'economia circolare e il ruolo dei consumatori nella protezione dell'ambiente: le nuove iniziative della Commissione UE*, in *Rivista giuridica dell'ambiente*, 2020, 4, 707-748.

[26] La Direttiva (UE) 2024/825, asse centrale della normativa europea sul contrasto alle pratiche ingannevoli, modifica le direttive 2005/29 (pratiche commerciali sleali) e 2011/83 (diritti dei consumatori), pubblicata sulla Gazzetta Ufficiale dell'Unione Europea il 6 marzo 2024, cfr. G. MARCATAJO, *Trasparenza del mercato, tutela del consumatore e greenwashing*, in *Jus vita e pensiero*, 2023.

[27] Trattasi di enti terzi autorizzati e accreditati (in Italia Accredia) per valutare i requisiti di legge del prodotto. In relazione all'ambito di riferimento variano le istituzioni addette alla verifica, per i prodotti regolamentati il riferimento è ad organismi notificati, per le dichiarazioni ambientali, le asserzioni di sostenibilità devono essere certificate da verificatori indipendenti accreditati secondo standard specifici (come la ISO 17033), per i sistemi di gestione vi sono enti certificatori privati (TUV, DQS) che validano le asserzioni aziendali (es. ISO14001). Riferimenti completi sono desumibili dal database NANDO della Commissione Europea.

[28] In Francia, l'Agenzia francese per la transizione ecologica, ed il Consiglio Nazionale dei Consumatori (CNC) hanno pubblicato, nel 2023, la 3a edizione della *Guida pratica alle asserzioni ambientali*. Consultabile online: https://infos.ademe.fr/magazine-novembre-2023/decryptage/on-ne-peut-pas-mettre-nimporte-quoi-sur-une-etiquette. Rilevante *la Loi Clima et Résilience* del 22 agosto 2021, sulla quale cfr. L. COLELLA, *La "transizione ecologica" nella Loi clima et résilience in Francia. Brevi note introduttive*, in *Contabilita-pubblica.it.* Per il Regno Unito il Green claims code in gov.uk. Per la Spagna si veda il *Codigo de autoregulacion sobre argumentos ambientales en comunicaciones comerciales in miteco.gob.es.*

coordinamento normativo, anche in relazione ad altre direttive (Corporate Sustainability Reporting Directive- CSRD, e la Corporate Sustainability Due Diligence Directive) [29]. Rilievi quest'ultimi che nel loro complesso hanno generato dubbi sulla efficacia complessiva dell'intervento.

4. Il ruolo dell'autodisciplina pubblicitaria nell'ordinamento italiano.

A fronte del protrarsi dell'impasse normativa europea, in Italia la tutela consumeristica avverso pratiche ingannevoli dal punto di vista del richiamo alla sostenibilità, si svolge su un piano marcatamente privatistico. Il riferimento è all'azione dispiegata dall'Istituto di Autodisciplina Pubblicitaria[30] (IAP), che sin dal 1966 con il Codice di Autodisciplina [31], aggiornato periodicamente, ha consentito la vigenza nell'ordinamento interno dell'abuso di dichiarazioni che richiamano la sostenibilità ambientale[32]. Più precisamente, l'assunto per cui «la

[29] A. TROISI, "*Cosa c'è dietro il ritiro della direttiva "Green Claims",* in *Energia e Ambiente, Imprese, Unione Europea,* 15/07/2025, *rivista on line*. In particolare sulle altre direttive *Corporate Sustainability Reporting Directive* (CSRD); cfr. A. GENOVESE, *L'armonizzazione del reporting di sostenibilità delle imprese azionarie europee dopo la CSRD*, in *Contratto e Impresa*, 2023, 88-111, l'autrice si sofferma sulla portata della standardizzazione europea, rilevando come l'adozione degli standard EFRAG (*European Financial Reporting Advisory Group* organismo europeo indipendente che fornisce consulenza tecnica alla Commissione Europea in materia di rendicontazione aziendale) limiti la discrezionalità alle imprese e consenta un confronto oggettivo tra società nel mercato capitalistico. Cfr. anche M. LIBERTINI, *Gestione "sostenibile" delle imprese e limiti alla discrezionalità imprenditoriale,* in *Contratto e Impresa*, 2023, 34-87.

[30] L'Istituto di Autodisciplina Pubblicitaria, associazione riconosciuta ai sensi dell'art. 14 c.c., fissa i parametri per una comunicazione commerciale onesta, veritiera e corretta a tutela dei consumatori e della leale concorrenza tra le imprese. L'obiettivo che l'Istituto persegue attraverso il Codice di Autodisciplina è la diffusione di una comunicazione commerciale responsabile, a vantaggio delle aziende, che richiedono il rispetto delle regole della concorrenza, dei cittadini-consumatori, che rifiutano messaggi ingannevoli o offensivi e dei mezzi di informazione. Per approfondimenti circa la considerazione dell'autodisciplina pubblicitaria nella dottrina cfr. V. MELI, *La repressione della pubblicità ingannevole (commento al DL n. 74 del 25 gennaio 1992)*, in *Quaderni di diritto commerciale europeo*, Torino, 1994, 210, in cui l'autore analizza i meccanismi normativi e giurisprudenziali volti a tutelare i consumatori e la concorrenza nel mercato. C. ALVISI, V. GUGGINO, *Autodisciplina pubblicitaria. La soft law della pubblicità italiana,* Torino, anche V. GUGGINO, *La dimensione europea dell'Autodisciplina Pubblicitaria. Il sistema autodisciplinare in Italia*, in Fogli di Lavoro per il Diritto Internazionale, 2015, 5-8. Consultabile online: http://www.lex.unict.it/it/crio/fogli-di-lavoro ed anche il lavoro monografico di M. REALE, *L'autodisciplina pubblicitaria in Italia. Teoria e prassi di un sistema normativo semiautonomo*, Milano 2022. Scritti che nel loro complesso dimostrano l'attendibilità delle tutele apprestate dal codice di autodisciplina anche nel giudizio di autorevole dottrina. V. GRAZZINI, *Norme preliminari e generali*, in AA. VV., *Commentario al Codice dell'Autodisciplina pubblicitaria*, a cura di U. RUFFOLO, Milano, 2003, 5; L. SORDELLI, *Voce Pubblicità (disciplina della)*, in *Enc. giur. Treccani*, vol. XXV, Roma, 1991, 3.

[31] Aggiornamenti significativi dello IAP vengono apportati il 14 febbraio 2014 ed entrano in vigore il 27 marzo 2014, per rafforzare la necessità di verità e correttezza nelle dichiarazioni pubblicitarie, proprio per contrastare esagerazioni, dichiarazione ambientali ingannevoli e testimonianze non veritiere. L'art. 12 bis intitolato alla «Sicurezza» che «la comunicazione commerciale relativa a prodotti suscettibili di presentare pericoli, in particolare per la salute la sicurezza e l'ambiente, specie quando detti pericoli non sono facilmente riconoscibili deve indicarli con chiarezza. Comunque, la comunicazione commerciale non deve contenere descrizioni o rappresentazioni tali da indurre i destinatari a trascurare le normali regole di prudenza o a diminuire il senso di vigilanza e di responsabiità verso i pericoli». Sulla natura giuridica dell'autodisciplina pubblicitaria cfr. A. PEDRIALI, *Natura giuridica dell'autodisciplina pubblicitaria*, in *Dir. Inf*. 1997, 594 che rinvia a R. FRANCESCHELLI, *Il nuovo codice di lealtà pubblicitaria*, in *Riv. dir. ind*. 1971, I, 319.

[32] Il codice di autodisciplina pubblicitaria è stato emanato per la prima volta 1l 12 maggio 1966 dall'istituto dell'Autodisciplina Pubblicitaria (IAP). Oggetto della codificazione è la regolamentazione della correttezza della pubblicità per la tutela del consumatore e delle imprese. Le principali associazione di categoria del settore (utenti, agenzie e mezzi di comunicazione si sono riuniti nell'istituto dell'autodisciplina Pubblicitaria). Le norme dell'IAP sono vincolanti per tutti i soggetti che volontariamente aderiscono e firmano contratti che implicano l'accettazione delle regole di correttezza nella comunicazione commerciale. Il sistema si avvale di un comitato di controllo e di un Giurì che giudica i messaggi contestati. Il testo del codice viene

comunicazione commerciale che dichiari o evochi benefici di carattere ambientale o ecologico deve basarsi su dati veritieri, pertinenti e scientificamente verificabili….deve consentire di comprendere chiaramente a quale aspetto del prodotto o dell'attività pubblicizzata i benefici vantati si riferiscono» (art.12) [33] è posto alla base dell'intervento inibitorio. Le autodiscipline pubblicitarie [34] hanno trovato esplicito riconoscimento anche nell'Unione Europea, che sin dagli anni 80', con la direttiva n. 1984/450/UE[35] sulla pubblicità ingannevole ha precisato che «controlli volontari esercitati da organismi autonomi per eliminare la pubblicità ingannevole possono evitare azioni giudiziarie o ricorsi amministrativi e devono quindi essere incoraggiati». In effetti, la stessa direttiva sulla pubblicità ingannevole e comparativa, n. 29 sin dal 2005[36], ne sottolinea la rilevanza[37]. Nel nostro ordinamento, i d.lgs. n. 145 e 146 del 2007[38] hanno legittimato l'autotutela pubblicitaria attraverso l'introduzione della sanzione autodisciplinare della tempestiva inibitoria relativa alla comunicazione ritenuta non conforme al codice, da espungere immediatamente dal sistema mediatico. Anche il codice del consumo riproduce espliciti riferimenti agli organismi volontari e autonomi di autodisciplina, con la

costantemente aggiornato per rispondere alle nuove sfide tecnologiche (digital chart per il marketing sui social media) e di mercato. L'ultima edizione risale ad ottobre 2024, 71 esima edizione in vigore dal 30 ottobre 2024. Per le origini, cfr. V. N. BOBBIO, *Diritto*, in *Noviss. dig. it.*, V, Torino, 1968, 774 ed anche M. FUSI, *Il nuovo Codice di lealtà pubblicitaria nella giurisprudenza del Giurì*, Milano, 1971, 30.

[33] Il Codice di Autodisciplina è vincolante per aziende che investono in comunicazione, agenzie, consulenti, mezzi di diffusione, concessionarie e per tutti coloro che lo abbiano accettato tramite la propria associazione, o mediante la conclusione di un contratto di inserzione pubblicitaria, cfr. S. POLIDORO, *Le sanzioni del codice di autodisciplina pubblicitaria,* in *Riv. dir. Ind.*, 1989, I, 61-62.

[34] Sul ruolo strutturale e organizzativo di sottosistemi sociali dell'autonomia privata e il ritirarsi della potestà regolativa eteronoma per la cieca fiducia nell'autoregolamentazione che riscrive una nuova teoria delle fonti contemplate dall'autonomia privata quale strumento strutturale di produzione di regole oggettive, operanti anche al di là della ristretta cerchia dei soggetti che le pongono cfr. F. CRISCUOLO, *L'autodisciplina, autonomia privata e sistema delle fonti,* Napoli, 2000, *passim.*

[35] Direttiva 1984/450/CEE del Consiglio del 10 settembre 1984 relativa al riavvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di pubblicità ingannevole, in G.U. n. L 250 del 19/09/1984, 17-20.

[36] Direttiva 2005/29/CE relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica le direttive 1984/450/CEE, 1997/07/CE, 1998/27/CE, per approfondimento dottrinario cfr. R. DI RAIMO, *Note minime sulle implicazioni sostanziali dell'art. 14 della direttiva 2005/29/CE: a margine di una proposta per il suo recepimento,* in *Contr. e impr./Europa*, 2007, II, 91 ss., anche P. BARTOLOMUCCI, *L'attuazione della direttiva sulle pratiche commerciali scorrette e le modifiche al codice del consumo, i*n *Rass. dir. civ.,* 2008, I, 269.

[37] In questi termini «è opportuno prevedere un ruolo per i codici di condotta che consenta ai professionisti di applicare in modo efficace i principi di trasparenza informativa in specifici settori economici. Il controllo esercitato dai titolari dei codici a livello nazionale o comunitario per l'eliminazione delle pratiche commerciali sleali può evitare la necessità di esperire azioni giudiziarie o amministrative e dovrebbe pertanto essere incoraggiato». Sul punto V. DI CATALDO*, Natura giuridica dell'autodisciplina pubblicitaria e ambito soggettivo di applicazione del Codice di Autodisci*plina, in *Contr. e impresa,* 1991, 120-121 che ritiene possibile utilizzare per la clausola di accettazione del codice il richiamo all'art. 1340 c.c., in assenza di contrasto delle parti contrattuali. Cfr. anche A. PEDRIALI, *Profili soggettivi dell'autodisciplina pubblicitaria* in *Riv. dir. Ind.*, I, 1992, 128 ss.

[38] I poteri di intervento del Giurì e del comitato di controllo non si limitano alle forme di pubblicità classica ma involgono anche le promozioni commerciali, le comunicazioni commerciali e tutte le forme di marketing in cui vi sia diretto coinvolgimento del pubblico. Sul punto cfr. la decisione del Giurì in data 2 dicembre 1987 n. 124/87 in Giur. Pubbl. I, 593 ss., in cui il Giurì rileva: «dopo che per vent'anni in tutti i contratti pubblicitari vengono inserite clausole sostanzialmente uniformi, ben può dirsi che tale accettazione abbia assunto il carattere di norma contrattuale consuetudinaria e che perciò ogni contratto pubblicitario oggi stipulato, ancorché in ipotesi non la contenga espressamente, comporti tale accettazione ai sensi dell'art. 1374 c.c.…». Per una rassegna dei casi trattati dal Giurì dal 1977 al 1985 cfr. L.C. UBERTAZZI, *Giurisprudenza completa del Giurì di autodisciplina pubblicitaria (1977-1985)*, Milano, 1986.

possibilità di chiedere, tra l'altro, la sospensione del procedimento innanzi all'Autorità, in attesa della pronuncia dell'organismo di autodisciplina. L'Istituto di Autodisciplina Pubblicitaria (IAP) nel campo della comunicazione commerciale, viene così ad appropriarsi del ruolo di interlocutore naturale dell'Autorità Garante della Concorrenza e del Mercato e nei casi che riguardano investimenti finanziari sostenibili può interagire anche con la CONSOB. L'art. 2 del codice del consumo, individua il parametro di valutazione della pubblicità ingannevole, come riferito soggettivamente al consumatore medio del gruppo di riferimento[39]. Anche gli organi giurisdizionali statali[40] hanno individuato nelle regole contenute nel Codice IAP, il valore di parametri di valutazione della correttezza e della deontologia professionale, applicabili all'evoluzione delle esigenze dell'attività imprenditoriale[41]. L'IAP nel 2016 ha elaborato per il settore moda la Digital Chart nell'intento di fissare con chiarezza e trasparenza i parametri di riferimento per il marketing nella moda anche on line. Tuttavia, il settore moda si è mosso in piena autonomia, la Camera Nazionale della Moda Italiana, ha stilato le "linee guida e regole interpretative per gli influencer", proprio con l'obiettivo di individuare le principali pratiche adottate dai brand selezionati in relazione all'attivismo fatto registrare sui social network, ciò non ha impedito che lo IAP intervenisse, laddove vi fossero messaggi comunicativi in contrasto con le disposizioni stilate[42]. In conclusione, al fine di conferire la

[39] Art. 2 codice del consumo: «La comunicazione commerciale deve evitare ogni dichiarazione o rappresentazione che sia tale da indurre in errore i consumatori, anche per mezzo di omissioni, ambiguità o esagerazioni non palesemente iperboliche, specie per quanto riguarda le caratteristiche e gli effetti del prodotto, il prezzo, la gratuità, le condizioni di vendita, la diffusione, l'identità delle persone rappresentate, i premi o riconoscimenti. Nel valutare l'ingannevolezza della comunicazione commerciale si assume come parametro il consumatore medio del gruppo di riferimento».

[40] Cass., 3 gennaio 2019, n. 5, ha sancito che i regolamenti interni e le procedure aziendali sono vincolanti per la società. Il principio così sancito viene articolato sia nel senso di rendere esplicita l'efficacia vincolante delle norme di autodisciplina e delle procedure interne aziendali anche se più restrittive rispetto alla legge. Ulteriore implicazione riguarda il collegio sindacale che ha il dovere di controllare il rispetto delle procedure interne; infine, nel senso della rilevanza delle best practices, in un'ottica di buone prassi aziendali la violazione di protocolli e procedure può integrare violazione dei doveri di amministrazione e controllo con conseguente rilevanza sanzionatoria della CONSOB. Cfr. *www.dirittobancario.it,* per ulteriori approfondimenti v. A. TONIOLO, *Vincolatività delle politiche di engagement e responsabilità civile degli esponenti aziendali rispetto a profili ESG*, in *Riv. dir. banc.*, 2021,3-47.

[41] Accanto ai riconoscimenti formali dell'Autodisciplina sia a livello comunitario che nazionale, va tenuto presente il protocollo d'intesa tra il Ministro per le Pari Opportunità e l'Istituto dell'Autodisciplina Pubblicitaria in relazione alla comunicazione commerciale con contenuti di genere, quello firmato con l'Associazione Nazionale Comuni Italiani (ANCI), per ampliare il controllo autodisciplinare sulle affissioni in modo più capillare e il Protocollo firmato con l'Autorità Garante per l'infanzia e l'adolescenza, per una maggiore tutela dei minori e per rendere ancora più responsabili i soggetti che operano nella comunicazione commerciale; nonché l'accordo quadro con l'Autorità per le Garanzie nelle Comunicazioni per un controllo più efficace sulla comunicazione commerciale e una maggior tutela del consumatore.

[42] Recente l'ingiunzione n. 12/26 del 18/5/2026 nei confronti di Philipp Plein International AG, per l'affissione del messaggio "Just the right amount of wrong. The Plein luxury hospitality, entertainment & property group" sul Plain hotel presso l'aeroporto di Malpensa. Il messaggio veicolato con un'immagine forte è stata ritenuta dall'Istituto di autodisciplina manifestamente contraria agli artt. 9 – Violenza, volgarità, indecenza e 10 – Convinzioni morali, civili, religiose e dignità della persona – del Codice di Autodisciplina della Comunicazione Commerciale. L'immagine mostra un uomo e una donna in abiti da sera, seduti sugli scalini di una scala. L'uomo afferra a mano piena la gola della donna che ha gli occhi chiusi, mentre il claim recita "Just the right amount of wrong. The Plein luxury hospitality, entertainment & property group". Nella fattispecie la forma prescelta per promuovere i servizi alberghieri , vede prevalere nella veicolazione del messaggio la violazione del disposto dell'art. 9 del Codice, secondo cui la «pubblicità non deve contenere affermazioni o rappresentazioni di violenza fisica o morale…» e dell'art. 10 che impone il rispetto «della dignità della persona in tutte le sue forme ed espressioni», laddove la pubblicità viene a basarsi su dinamiche

giusta collocazione sistematica all'autodisciplina pubblicitaria è opportuno rilevare che autorevole dottrina, sin dalla prima fase applicativa colloca il sistema di autodisciplina pubblicitaria nell'ambito dell'ordinamento dei privati come tassello del pluralismo ordinamentale[43].

5. La direttiva 2024/825/UE e la tutela del consumatore.

Al di là della ingannevolezza della pubblicità, la Direttiva 2024/825/UE, "Empowering Consumers for the Green Transition", rappresenta la misura di contrasto al greenwashing e rafforza il focus esplicito sulla tutela del consumatore che diviene attore della svolta per l'affermazione della sostenibilità ambientale nel mercato attraverso le sue scelte di consumo informate, trasparenti e consapevoli. Rilevante è senz'altro l'individuazione di quelle dichiarazioni ambientali fuorvianti consistenti non solo in parole, marchi e loghi, ma anche in immagini evocative, colori, musiche e paesaggi che trasmettano il senso della tutela globale. Tra le pratiche vietate vi è l'uso di espressioni vaghe, come "verde" o "rispettoso dell'ambiente", quando non accompagnate da specifiche indicazioni oggettivamente verificabili. Sono inoltre proibiti loghi o simboli di sostenibilità privi di un reale sistema di certificazione o non riconosciuti da enti pubblici. Non sono consentite espressioni che facciano intendere un impatto positivo dell'intero prodotto quando, in realtà, riguardano solo un elemento specifico, come l'imballaggio. Anche le diciture "carbon neutral" non possono basarsi unicamente su compensazioni di quote di emissione, ma devono derivare da una reale certificata riduzione delle emissioni. Le dichiarazioni non chiare sulla durata del prodotto o sulla possibilità di essere riparato, così come l'esaltazione di elementi che in realtà rispecchiano solo requisiti minimi obbligatori sono vietate. La previsione dell'art. 2 della direttiva 2024/825/UE, modifica anche la direttiva 2011/83/UE, con specifico riferimento alla garanzia commerciale di durabilità, in base alla quale il produttore è responsabile direttamente nei confronti del consumatore per la riparazione o sostituzione dei beni nell'arco di tutta la durata della garanzia commerciale di durabilità in conformità all'art. 14 della direttiva 2019/771/UE. Quest'ultima previsione lascia trasparire la volontà legislativa di dare impulso alla transizione da un modello di economia lineare a quello circolare. Il parlamento europeo interviene su due piani. Sul piano dell'efficacia della nuova normativa sulla situazione esistente nel mercato, attraverso il divieto di pratiche ingannevoli; in relazione invece alla edificazione di una nuova sostenibilità in una prospettiva futura, la direttiva intende conferire centralità all'"avviso armonizzato" e all'"etichetta armonizzata". Il primo è obbligatorio, l'etichetta armonizzata che intende garantire ai consumatori le informazioni minime necessarie in tutti i paesi dell'Unione è invece strumento volontario, ciò che affievolisce la portata della

di predominio e violenza, la pubblicità è stata oggetto di ingiunzione e sanzionata con la immediata cessazione.

[43] In tal senso W. CESARINI SFORZA, *Il diritto dei privati*, Milano, 1963; S. ROMANO, *L'ordinamento giuridico*, Firenze, 1946; F. MODUGNO, *Pluralità degli ordinamenti* in *Enc. Dir., XXXIV,* Milano 1985, concordi nel sostenere che la teoria pluralista viene a fondarsi proprio sulla coesistenza tra ordinamenti tra loro differenti nell'ambito dell'unicità sociale di riferimento.

previsione. Il termine fissato dall'Unione Europea per il recepimento da parte dei singoli Stati membri, è il 27 marzo 2026, mentre alle imprese è assegnato il termine di settembre dello stesso anno per conformarsi pienamente alle nuove disposizioni. [44] L'art. 22 bis introduce l'obbligo negli Stati Membri dell'apposizione di un avviso che informi i consumatori sui loro diritti relativamente alla garanzia legale di conformità dei beni oggetto di vendita, sulla durata minima di due anni[45] e sull'eventuale possibilità che la garanzia si protragga anche oltre. È da rilevare come l'efficacia delle nuove misure sia rimessa a ulteriori atti normativi e come non vi sia una forte leva dal punto di vista sanzionatorio. *Rebus sic stantibus*, diviene significativa l'attuazione che gli Stati Membri daranno al profilo sanzionatorio in caso di violazione delle disposizioni anzidette.

6. Il greenwashing e la configurabilità del danno alla sostenibilità.

In tale quadro normativo, nei casi in cui i brands basino la loro politica di marketing sul greenwashing, con informazioni non veritiere sull'impatto ambientale della produzione o nelle etichette dei loro prodotti, potrebbero configurarsi varie tipologie di danni in correlazione alle diverse tipologie di rischi[46]. In primis il rischio reputazionale, ossia rischio che l'azienda possa subire un danno all'immagine e una perdita di credibilità; il rischio finanziario, che possa derivare dalle eventuali spese legali e/o sanzioni, ma anche dalla svalutazione dei titoli in borsa e dalla perdita di clienti o di quote di mercato; nonché il rischio legale connesso al sostenimento di oneri derivanti da un'obbligazione restitutoria o risarcitoria o dal subire sanzioni per la mancata applicazione delle normative sulla sostenibilità [47] . È evidente come l'informazione veicolata sortisca effetti nel sistema finanziario, oltre che nelle scelte del consumatore e, se erronea, possa generare asimmetrie e ledere l'interesse pubblico al corretto funzionamento dei meccanismi di formazione dei prezzi. È stato acutamente rilevato come Il danno che si produce per effetto di una informazione falsa o inesatta diffusa nel mercato finanziario si svolga lungo due direttrici, sia come danno al mercato, da intendersi come lesione dell'interesse pubblico al corretto funzionamento dei meccanismi di corretta formazione dei prezzi e, dall'altro e contemporaneamente, sebbene in via indiretta, come lesione del diritto di ogni singolo investitore di poter fare affidamento nel corretto funzionamento del mercato» [48] . È interessante, dunque chiedersi se, in queste fattispecie, sia possibile applicare la disciplina civilistica del danno a tutela dei soggetti lesi. Invero, il quesito non può

[44] La Direttiva 2024/825/UE va a modificare le direttive 2005/29/UE e la direttiva 2011/83/UE.
[45] Previsione presente nella Direttiva 2011/83/UE.
[46] Nel Forum per la finanza sostenibile, Greenwashing e finanza sostenibile: rischi e risorse di contrasto (in https://finanzasostenibile.it/wp- content/uploads/2022/11/Greenwashing_ITA_WEB.pdf) si configura il c.d. litigation risk, che consiste nel rischio che un individuo o una società possa dover affrontare un'azione legale, con l'espressione "ESG litigation risk" ci si riferisce, invece, al rischio che un individuo o una società debba subire un'azione legale correlata alla sostenibilità.
[47] Esempio di contenzioso connesso in senso stretto al greenwashing finanziario, considerate le ricadute anche *latu sensu* finanziarie, correlato a SFDR, è costituito, senz'altro, dal caso Volkswagen: cfr. G. MARCATAJO, *Trasparenza del mercato, tutela del consumatore e greenwashing*, in *Jus vita e pensiero*, 2023, 184.
[48] V. CARIDI, *Danno e responsabilità da informazione al mercato secondario*, Milano, 2012, 132.

prescindere da una riflessione sulla qualificazione giuridica della sostenibilità. Può quest'ultima ritenersi assurta a rango di diritto soggettivo assoluto? La risposta positiva consentirebbe il ricorso alla tutela aquiliana ex art. 2043 c.c.. Se, viceversa, la sostenibilità venga interpretata a livello costituzionale quale indicazione programmatica, allora l'efficacia della tutela risarcitoria diviene più labile e richiede una gradualità di approccio, parallelamente alla realizzazione del programma. A sommesso parere di chi scrive l'introduzione della sostenibilità[49] nella carta costituzionale, attraverso le modifiche degli artt. 9 e 41 cost. [50] , ben può legittimare la possibilità di delineare il "danno reputazionale" quale "sanzione civilistica", conseguente all'eventuale diffusione di informazioni non corrette e fuorvianti relativamente al prodotto o al processo di produzione. In questi termini, affermare che il greenwashing leda gravemente la sostenibilità costituzionale solennizzerebbe i doveri di solidarietà e la salvaguardia delle generazioni future anche in ambiti che sembrerebbero rilevanti solo per il marketing. Alla luce delle considerazioni svolte, la violazione dell'art. 9 cost., ipotizzata in fattispecie di greenwashing, non è mera astrazione nella misura in cui la tutela dell'ambiente, della biodiversità e degli ecosistemi venga inficiata da politiche di mercato che ingenerano una situazione di apparente rispetto ecologico e nella sostanza si risolvono in consapevoli violazioni dell'interesse pubblico alla sostenibilità a vantaggio di scopi privatistici meramente lucrativi. È riscontrabile altresì, la lesione della libertà di iniziativa economica (art. 41) nella misura in cui la prassi di ambientalismo solo proclamato e non praticato, fa sì che l'economia venga a svolgersi in contrasto con l'utilità sociale e in modo da recare danno alla salute e all'ambiente. Il greenwashing incide anche sull'andamento del mercato nella misura in cui altera il gioco della concorrenza, arreca vantaggio a chi finge di porre in essere un'attività sostenibile senza investire in tal senso. Anche il diritto dei consumatori all'informazione veritiera può ritenersi leso nelle suddette fattispecie (art. 21 Cost.). In sintesi, ricorre sovente la violazione di diritti soggettivi assoluti proclamati dalla nostra carta costituzionale, ciò che consente di configurare il danno ai consumatori e al mercato come fonte di responsabilità aquiliana.

7. Responsabilità negoziale e greenwashing.

Non meno opportuno è il richiamo alla responsabilità di natura negoziale precontrattuale e contrattuale. Nella misura in cui la prassi si sostanzi nella

[49] Può senz'altro ritenersi introdotta in modo esplicito con la riforma costituzionale del 2022 legge n1, pubblicata in G. U. 22 febbraio 2022 n. 44, che ha modificato gli artt. 9 e 41 cost., norme fondamentali per la tutela dell'ambiente dell'economia e le generazioni future

[50] In particolare, al'art. 9 Cost. è stata aggiunta la tutela dell'ambiente, della biodiversità e degli ecosistemi anche nell'interesse delle future generazioni). Sulla modifica cfr., *ex plurimis*, R. BIFULCO, *La legge costituzionale 1/2022. Problemi e prospettive,* in *Ann. giur. econ.*, 2022, 7 ss.; M. CECCHETTI, *Virtù e limiti della modifica degli articoli 9 e 41 della Costituzione,* in *Corti supreme e salute*, 2022, 127 ss.; G. MARCATAJO, *La riforma degli articoli 9 e 41 della Costituzione e la valorizzazione dell'ambiente,* in *Amb. dir.,* 2022, 118 ss.; U. MATTEI, *Qualche riflessione critica sulla svolta ecologica della Costituzione italiana,* 2022. Consultabile online: https://generazionifuture.org/qualche-riflessione-critica-sulla-svolta-ecologica-della-costituzione-italiana/; M.P. POTO, *La tutela costituzionale dell'ambiente, della biodiversità e degli ecosistemi, anche nell'interesse delle future generazioni*, in *Resp. civ. prev.*, 2022, 1057 ss.

violazione degli obblighi di correttezza e trasparenza sul mercato rispettivamente nella fase della trattativa può dar luogo a responsabilità precontrattuale. In ambito finanziario è richiamabile l'art. 94 del D. Lgs. 58/98 per cui gli investitori possono chiedere il risarcimento del danno all'emittente di un prodotto finanziario nel caso in cui il prospetto informativo contenga informazioni non veritiere o fuorvianti sul prodotto. Tale disposizione ben può essere invocata per avanzare richieste risarcitorie a fronte del danno derivante da dichiarazioni ingannevoli sulle credenziali "verdi" o ecologiche di un prodotto di impact financing. L'onere di provare i presupposti risarcitori (comportamento dannoso dell'emittente, danno, elemento soggettivo - dolo o colpa dell'emittente - e il nesso di causalità ricadrà sul danneggiato. o contrattuale quale inadempimento delle promesse ambientali nello svolgimento del rapporto. Nella fase della formazione del contratto, può senza dubbio essere rilevante la statuizione legislativa della necessità per il produttore dell'assolvimento di un obbligo informativo che incida sulla scelta del consumatore. La responsabilità contrattuale *ex* art. 1218 cod. civ., richiamabile quando una dichiarazione o un'affermazione contenuta in un contratto si riveli non veritiera, ben può attagliarsi alla fattispecie in esame. In ambito finanziario la norma potrebbe essere invocata da un investitore in relazione alle vantate credenziali di sostenibilità green. In questo caso, l'onere della prova spettante all'investitore si limiterebbe alla dimostrazione dell'esistenza del contratto (contenente le dichiarazioni non veritiere) e dei danni subìti. Il silenzio è giuridicamente irrilevante, a meno che la legge non ricolleghi conseguenze al medesimo, rendendolo significativo anche per la relativa omissione. Questo a tutela della libertà di scelta individuale. L'imposizione normativa di obblighi informativi e le relative sanzioni per la violazione può compensare l'asimmetria informativa originaria e precedente alle scelte di investimento, limitando lo squilibrio tra le parti[51]. In particolare, lo squilibrio può essere di tipo economico, quale sproporzione delle prestazioni, o normativo, nella misura in cui faccia riferimento ad un contenuto normativo nella disciplina contrattuale del rapporto. Nel caso in cui l'asimmetria informativa sia di carattere normativo, l'introduzione di tale obbligo da parte del legislatore, ben può rivelarsi essenziale al fine di arginare la condizione di debolezza contrattuale. Deve tuttavia trattarsi di un'asimmetria "qualificata" ed occorre trovare un equilibrio tra il dovere di informazione e l'"opportunistico" silenzio[52]. Nella dinamica contrattuale reale, infatti, la parte che è in possesso di maggiori informazioni è portata a evitare di farle conoscere alla controparte, che potrebbe volgerle a suo svantaggio. Il settore della moda, in particolare, evidenzia frequentemente pratiche associabili al "greenwashing" entrato nell'etica consumeristica sia dei consumatori finali, come anche delle organizzazioni a tutela dei loro diritti e delle autorità di regolamentazione della concorrenza. Paradossalmente, questo rinnovato interesse ha alimentato anche la diffusione di pratiche pubblicitarie ingannevoli, in quanto si è attivato un abuso del termine "green", che causa incertezze per i consumatori nel discernere tra comportamenti effettivamente responsabili e pratiche pubblicitarie ingannevoli. A livello processualistico è

[51] G. Grisi, *Informazione (obblighi di),* in *Enc. dir.*, IV, Milano, 2011, 595-627.
[52] G. Grisi, *op. loc. cit.*, 600, nt. 33.

opportuno il riferimento all'esperibilità dell'azione di classe in seguito ai significativi ampliamenti conseguenti alle riforme *ex* l. 12 aprile 2019, n. 31[53] e *ex* d. lgs. 10 marzo 2023, n. 28 a seguito dell'attuazione della Direttiva (UE) 1828/2020.

Alla luce del quadro delineato è di immediata evidenza come la Direttiva Greenwashing UE (n. 825/2024), rappresenti il tassello evolutivo fondamentale per il contrasto a fenomeni basati su falso ambientalismo commissivi o omissivi idonei ad alterare sia il meccanismo di formazione del consenso tra le parti che l'andamento del mercato.

8. Altre fattispecie sanzionatorie per arginare il greenwashing.

La dimensione ambientale ben può diventare parte integrante della veridicità complessiva dell'informazione societaria al punto di trasformare il greenwashing in reato societario (artt. 2621-2622 c.c.). In ambito penalistico è assente la configurazione della prassi anzidetta come reato autonomo, tuttavia le fattispecie di pratiche di finta sostenibilità divengono penalmente rilevanti come fatti che integrano la frode in commercio e il falso in bilancio, nella misura in cui l'ingannevolezza si concretizzi in un vantaggio economico ingiusto o in comunicazioni societarie mendaci[54]. Le dimensioni interdisciplinari rendono l'ampiezza distorsiva del fenomeno a ben vedere non più limitata al piano civilistico della pubblicità ingannevole, ma estesa sino ad alterare la veridicità

[53] Per effetto dell'abrogazione degli artt. 139,140, e 140 bis del codice del consumo relativi all'azione inibitoria e alla c.d. azione di classe, con l'effetto di estendere l'ambito applicativo delle azioni collettive, come concepite nel codice del consumo sia da un punto di vista oggettivo che soggettivo, a seguito dell'inserimento del titolo VIII bis "dei procedimenti collettivi", nel libro IV del codice civile, per cui l'azione di classe può ora essere intentata da chiunque intenda far valere "diritti individuali omogenei" (e non è quindi più limitata – come avveniva in passato – alla tutela dei diritti del "consumatore" o "utente" secondo le disposizioni del Codice del Consumo). Inoltre, in seguito all'emanazione del d. lgs. d. lgs. 10 marzo 2023, n. 28 attuativo della Direttiva (UE) 1828/2020 è stato realizzato l'intento di assicurare una tutela effettiva ed uniforme dei diritti dei consumatori anche a livello europeo. Attualmente quindi è previsto un doppio binario: da un lato l'azione rappresentativa nazionale e transfrontaliera disciplinata dal codice del consumo esperibile da parte degli enti legittimati ad agire per la tutela degli interessi dei consumatori in relazione a disposizione specificamente individuate; dall'altro i procedimenti collettivi di cui al codice di procedura civile, esperibili senza una restrizione per materia tanto da associazioni o organizzazioni quanto autonomamente da ciascun membro appartenente alla stessa classe. Peer approfondimento cfr. F. CESAREO, G. PIROTTA, *Il greenwashing nella lotta al climate change. Fondamenti sostanziali giusprivatistici e tutela risarcitoria collettiva*, in *BioLaw Journal - Rivista di BioDiritto*, 2023, 2.

[54] G. D'IPPOLITO, *Greenwashing: ecco quando la finta sostenibilità diventa illecito penale*, in *Responsabilità d'impresa,* in *Network 360*, 17.12.2025. Consultabile al sito: https://www.agendadigitale.eu/smart-city/greenwashing-ecco-quando-la-finta-sostenibilita-diventa-illecito-penale/. L'Europa e l'Italia ridisegnano la responsabilità d'impresa sulla verità delle dichiarazioni ambientali, Frode in commercio (Art. 515 c.p.): si configura quando si vende un prodotto dichiarandolo "ecologico" o "riciclato" ma fornendo in realtà beni di qualità e caratteristiche ambientali diverse da quelle pattuite, inganno sul prodotto. Dal punto di vista soggettivo è richiamabile la fattispecie della vendita di prodotti industriali con segni mendaci (art. 517 c.p.), punisce chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto. Truffa (art. 640 c.p.), quando la menzogna verde serve a ottenere vantaggi economici, come contributi pubblici o premi ambientali, in forma aggravata (art. 640-bis c.p.), quando serve al conseguimento di fondi pubblici (es. PNRR, incentivi green).ma anche richiamabile e applicabile qualora l'inganno ambientale causi un danno patrimoniale diretto a investitori o acquirenti. Falso in bilancio (Art. 2621 o 2622 c.c.): le dichiarazioni ingannevoli sulla sostenibilità (ESG) inserite nelle relazioni finanziarie possono integrare questo reato se alterano la percezione della salute economica dell'impresa. truffa (Art. 640 c.p.): applicabile qualora l'inganno ambientale causi un danno patrimoniale diretto a investitori o acquirenti.

dei dati contenuti in documenti che fanno fede al pubblico quali i bilanci di sostenibilità delle imprese, nei rapporti ESG, nelle dichiarazioni non finanziarie e nelle etichettature dei prodotti[55].

9. La falsa dichiarazione oltre la sostenibilità nei rapporti con la pubblica amministrazione.

Anche fattispecie di falsità documentali e comunicazioni ambientali che incidono nei rapporti con la pubblica amministrazione possono configurare la falsità ideologica in atto pubblico (art. 479 c.p.), nel caso in cui un pubblico ufficiale attesti in un atto pubblico contenuti ambientali (es. autorizzazioni, verbali) non veritieri e falsità materiale commessa da privato (art. 482 c.p.), (es. certificazioni ambientali).In tale fattispecie ricorre la comunicazione ambientale falsa, riconducibile all'art. 258 del codice dell'ambiente (D.lgs. 152/2006), così come nell'iter procedurale di rilascio di Autorizzazione Integrata ambientale (AIA), VIA (valutazione di impatto ambientale), autorizzazioni, CAM (art. 57, co. 2, D.lgs. 36/2023). In questi casi la falsa manifestazione ambientale o la falsa dichiarazione possono incidere direttamente sul corretto esercizio del potere autorizzatorio e sulla tutela effettiva dell'ambiente, quali reati ambientali (art. 452 bis D.lgs. 152/2006 e L. 68/2015) anche talvolta rappresentabili come circostanze aggravanti o elementi strumentali per altri reati ambientali, come il disastro ambientale colposo o doloso, l'inquinamento ambientale o la gestione illecita dei rifiuti[56].

10. Provvedimenti giurisdizionali a tutela del mercato e del consumatore.

A livello applicativo, i rilevanti interventi legislativi fanno annoverare una particolare incisività degli interventi dell'AGCM, in ambito moda[57] e logistica di

[55] Cass., Sez. Unite, 27.05.2016, n. 22474, che conferma la rilevanza penale del falso "valutativo" nelle false comunicazioni sociali; principio spesso richiamato quando i claim ESG entrano in documenti societari.

[56] Cass. Pen., sez. III, 05.04.2019, n. 15011, sul falso ideologico in autorizzazioni amministrative (art. 480–479 c.p.), principi utilizzati anche nei procedimenti su nulla osta/permessi con profili ambientali o paesaggistici. Cass. Pen., sez. III, 28.11.2019, n. 48401, sui reati ambientali in tema di A.I.A. e sugli obblighi di controllo/comunicazione e responsabilità per omissioni o dati non veritieri.

[57] L'Autorità Garante della Concorrenza e del Mercato - sanzione di 1 milione di euro a Shein per green claim ingannevoli e omissivi a Infinite Styles Services Co. Ltd, società che in Europa gestisce i siti di compravendita dei prodotti Shein, per l'utilizzo di messaggi e asserzioni ambientali (green claim) ingannevoli/omissivi nella promozione e vendita di prodotti di abbigliamento a marchio Shein..Le asserzioni ambientali che hanno portato l'Authority ad irrogare la sanzione sono contenute nella sezione #SHEINTHEKNOW, e fanno riferimento proprio ad una sorta di knowhow sulla circolarità e riciclabilità dei prodotti, espresse in termini di progettualità. Tuttavia, le asserzioni sono risultate false o quanto meno fuorvianti. In particolare, i claim utilizzati da Shein per valorizzare i capi di abbigliamento della linea "evoluSHEIN by Design" enfatizzano l'uso di fibre "green" senza indicare i sostanziali benefici ambientali dei prodotti e senza rilevare che tale linea di prodotti è marginale rispetto alla maggioranza di prodotti a marchio Shein, privi delle caratteristiche ambientali enfatizzate. La "mistificazione consumeristica" è chiara le green claims ben possono indurre i consumatori a ritenere che la linea "evoluSHEIN by Design" sia realizzata unicamente con materiali "ecosostenibili", e siano totalmente riciclabili, qualità quest'ultima che, con riferimento alla composizione delle fibre utilizzate nel processo produttivo e i sistemi di riciclo attualmente esistenti, non risulta veritiera. A questa mistificazione si aggiunga l'annuncio da parte di Shein di un programma di riduzione del 25% delle emissioni di gas serra entro il 2030 e di azzerarle entro il 2050, proclama quest'ultimo enunciato i, nella sezione dedicata alla "Responsabilità sociale". A bene vedere le emissioni di gas serra dell'attività di Shein

supporto al settore[58], che colpiscono patrimonialmente le pratiche commerciali scorrette [59] con ulteriore effetto di monito [60] per il mercato in generale. È questa la sanzione più efficace, ben oltre la semplice inibitoria. L'Agcm sembra abbia valutato la fattispecie con particolare severità, anche in ragione del fatto che «il trasporto delle merci è uno dei settori economici maggiormente inquinanti, che richiede particolare rigore e accuratezza alle imprese che vi operano e che decidono di promuovere la propria attività facendo leva sulle iniziative di sostenibilità ambientale (c.d. "green appeal")». L'Autorità ha rigettato gli impegni proposti dal Gruppo GLS per ottenere la chiusura del procedimento senza l'accertamento dell'infrazione "a causa della manifesta gravità e dell'elevato grado di offensività delle condotte contestate, anche in ragione del crescente interesse da parte di consumatori e imprese nei confronti

nel biennio 2023-2024 fanno registrare un incremento. Per approfondimenti dottrinari cfr. V. PICCININI, *Il contrasto al greenwashing nel settore del fast fashion: l'"AGCM sanziona Shein*, in rivista di diritto del risparmio, 2025, 3.

Nel valutare la scorrettezza delle condotte di Shein, l'Autorità ha evidenziato il maggior dovere di diligenza che incombe su di essa perché opera in un settore e con modalità altamente inquinanti, come quello dell'abbigliamento cosiddetto "usa e getta" ("*fast e super fast fashion*").

[58] Altro caso di intervento dell'AGCM è relativo alla Armani, che ha subito l'irrogazione di una multa di 3,5 milioni di euro per pratiche commerciali scorrette e dichiarazioni non veritiere sulla responsabilità sociale e sul rispetto dei diritti dei lavoratori nella filiera.

[59]Per approfondimento del ruolo strategico, rivestito dalla regolamentazione delle modalità di svolgimento delle attività svolte dagli operatori economici e i limiti della sostenibilità solo conclamata ai fini della costruzione di un futuro sostenibile nella consapevolezza della stretta correlazione esistente tra tutela del mercato, tutela del consumatore in linea con la disciplina delle pratiche commerciali scorrette cfr. S. TOMMASI, *Pratiche commerciali scorrette e disciplina dell'attività negoziale*, Bari, 2012, 24; G. GRISI, *Rapporto di consumo e pratiche commerciali*, in *Europa e diritto privato*, 2013, 1 ss.

[60] Recente il caso trattato il 21 gennaio 2025 dall'AGCM che ha portato all'irrogazione a varie società del Gruppo GLS ("GLS"), attivo nella spedizione, trasporto e consegna di merci, una sanzione di 8 milioni di euro per pratiche commerciali, ingannevoli e aggressive, incentrate su vanti ambientali ambigui, non accurati e non verificabili In estrema sintesi, GLS ha adottato un progetto di sostenibilità ambientale denominato "Climate Protect", in forza del quale si proponeva, tra l'altro, di utilizzare energia verde nelle proprie strutture, impiegare veicoli per le consegne "a zero emissioni", realizzare edifici secondo elevati standard di sostenibilità e compensare le emissioni di CO2 del network GLS. Tali iniziative sono state ampiamente pubblicizzate, anche tramite il sito internet, presso i consumatori, le imprese clienti e le aziende di trasporto affiliate al network di GLS (molte delle quali considerate "micro-imprese"). Secondo l'Autorità, i messaggi: (i) non consentivano di comprendere la profonda differenza tra attività di "compensazione" e attività di "riduzione" delle emissioni, lasciando intendere che le prime fossero idonee a "rendere meno inquinanti i servizi di spedizione offerti da GLS"; (ii) facevano riferimento a un certificato di compensazione non ancora ottenuto alla data della loro diffusione; (iii) contenevano dati non corretti o incompleti. Ad esempio, le informazioni necessarie per decodificare i claim "100% energia verde nelle nostre strutture" e "veicoli per le consegne a zero emissioni" non erano fornite in prossimità degli stessi, ma erano necessari "parecchi scroll della pagina web". Inoltre, tali informazioni sono state giudicate non puntuali, stante il fatto che le percentuali di strutture alimentate a energia verde e di veicoli elettrici utilizzati risultavano essere molto più contenute di quelle indicate nelle note (che già ridimensionavano significativamente i vanti ambientali contenuti nei claim).Per di più, in merito alla contestazione circa la non chiara distinzione tra "compensazione" e "riduzione delle emissioni", il principio che dette attività non siano equivalenti e non possano essere confuse nella comunicazione è ben consolidato ed è stato cristallizzato dal legislatore europeo nella direttiva n. 2024/825 del 28 febbraio 2024 (su cui si tornerà a breve) che ha ricondotto a una fattispecie di pratica commerciale scorretta ingannevole "Asserire, sulla base della compensazione delle emissioni di gas a effetto serra, che un prodotto ha un impatto neutro, ridotto o positivo sull'ambiente in termini di emissioni di gas a effetto serra". Tornando al provvedimento, oltre a quanto sopra, diversamente da quanto dichiarato e con decisione unilaterale, GLS avrebbe traslato integralmente il costo del progetto *Climate Protect* su determinate imprese clienti e affiliate. In pratica, ciascuna impresa si sarebbe vista imporre un contributo a fronte del rilascio di un certificato, non richiesto, attestante la compensazione di CO2 riconducibile alla medesima impresa. Peraltro, detti certificati sono risultati inattendibili, in quanto basati su valori medi nazionali anziché su dati specifici delle singole imprese.

della tematica dei claims ambientali"[61], ciò che acclara la responsabilità per claim ambientale privo di certificazione, sanzionata con la condanna per concorrenza sleale, giudicato allineato alla giurisprudenza europea[62], sui green claims fuorvianti come pratica scorretta.

11. Il contrasto all'obsolescenza programmata.

Sempre riconducibile ad una omissione informativa è la ratio insita nel fenomeno dell'obsolescenza programmata. Prassi quest'ultima invalsa presso talune multinazionali volte ad incidere sulla durata di vita utile del prodotto. Aspetto considerato dalla Commissione europea come pratica ingannevole nell'ambito della direttiva 2024/825 (considerando16,17,18). Immediato il riferimento a beni la cui durata può essere gestita direttamente dal produttore con accorgimenti tecnici limitativi finalizzati ad accrescerne il consumo. L'esempio più ricorrente di obsolescenza programmata è collegato all'aggiornamento dei software che dietro il dichiarato proposito di migliorare le prestazioni in realtà ne compromette la durata sino ad arrivare ad un vero e proprio blocco di funzionamento dei device (es. cellulari)[63]. Il fenomeno distorsivo viene considerato tra le pratiche commerciali ingannevoli che trovano regolamentazione nella direttiva 825/24[64].

Peraltro, l'obsolescenza precoce incide complessivamente sull'ambiente nella misura in cui determina un aumento dei rifiuti e un maggiore utilizzo di energia e materiali. L'invito del Parlamento europeo nella direttiva 825/24 è nel

[61] Tra i primi interventi giurisdizionali in Italia e in Europa, nel contrasto al fenomeno del greenwashing è annoverabile l'ordinanza cautelare emessa dal Tribunale di Gorizia del 26 novembre 2021 che ha accolto il ricorso legale presentato da Alcantara S.p.A. contro Mirko S.r.l, rispettivamente due società umbre e friulane operanti nel settore tessile, chiedendo l'inibitoria immediata della diffusione di determinati messaggi pubblicitari emessi, ritenuti quest'ultimi ingannevoli e veicolati attraverso canali di comunicazione online e offline. In particolare, Mirko S.r.l aveva descritto una microfibra come "ecosostenibile", senza tuttavia fornire prove concrete a supporto di tale affermazione. In tale pronuncia il Tribunale ha qualificato "eccessivamente generici" i messaggi pubblicitari esaminati, i quali risultavano idonei a creare nella mente del consumatore l'illusione di una connotazione ecologica e sostenibile dell'impresa. Il giudice ha, pertanto, inquadrato la vicenda nell'ambito della concorrenza sleale (ai sensi dell'art. 2598 c.c.) e nell'ambito della pubblicità ingannevole (ai sensi del decreto legislativo n.145 del 2007, in attuazione dell'art. 14 della Direttiva 29/2005/CE), sottolineando che l'uso di tali asserzioni ecologiche conferiscono un vantaggio competitivo all'impresa che lo adotta, dal momento che possono influenzare significativamente le decisioni di acquisto del consumatore. Pertanto, il giudice ha stabilito una penalità per ogni giorno di ritardo nell'esecuzione del provvedimento, obbligando l'azienda a notificare l'ordinanza a tutti i propri clienti e a pubblicarla sulla homepage del proprio sito per un periodo di 60 giorni consecutivi.

[62] Corte di Giustizia UE, causa C-388/20, sulla trasparenza e la pubblicità ambientale, e causa C-632/16, sulle informazioni ambientali fuorvianti come pratica sleale.

[63] Casi storici ad esito di due complesse istruttorie hanno portato l'AGCM ad accertare che le società del gruppo Apple e del gruppo Samsung hanno realizzato pratiche commerciali scorrette in violazione degli artt. 20, 21, 22 e 24 del Codice del Consumo in relazione al rilascio di alcuni aggiornamenti del firmware dei cellulari che hanno provocato gravi disfunzioni e ridotto in modo significativo le prestazioni accelerando il processo di sostituzione degli stessi. Alle due imprese sono state applicate sanzioni pari al massimo edittale, tenuto conto della gravità delle condotte e della dimensione dei professionisti: a Samsung 5 milioni di euro e ad Apple 10 milioni di euro (5 milioni per ciascuna delle due pratiche contestate). Entrambe le imprese dovranno inoltre pubblicare sulla pagina in italiano del proprio sito internet una dichiarazione rettificativa che informi della decisione dell'Autorità con il link al provvedimento di accertamento. Nel corso dell'attività ispettiva, i funzionari dell'Autorità Garante della Concorrenza e del Mercato si sono avvalsi dell'ausilio del Nucleo speciale Antitrust della Guardia di Finanza.

[64] Rilevanti i considerando 16, 17 e 18 della direttiva 825/24 che evidenziano la necessità di modificare la direttiva 29/2005, per il contrasto a prassi di obsolescenza programmata.

senso di favorire il miglioramento della comunicazione ai consumatori relativamente agli effetti che un determinato aggiornamento del software potrà avere sul funzionamento di beni che comprendono elementi digitali o sull'uso di contenuti digitali o servizi digitali.

È rilevante che il divieto si applichi a qualsiasi aggiornamento, compresi quelli di sicurezza e relativi alla funzionalità necessaria per mantenere la conformità dei beni, dei contenuti digitali e dei servizi digitali.

Il fenomeno dell'obsolescenza programmata potrebbe, sebbene in termini atipici, essere ipotizzato anche nel settore tessil/moda. Qualora la politica di produzione e vendita di un'azienda punti sul c.d. fast fashion[65], viene in rilievo la componente psicologica che porta il consumatore ad acquistare un capo dal prezzo basso, di infima qualità e di gran tendenza stilistica. Attraverso il fast fashion i *brand* spingono ad un consumo ciclico costante grazie all'induzione del desiderio di cambiare continuamente seguendo le tendenze più nuove[66]. L'obsolescenza nel settore moda[67] si configura in forma "subliminale" indotta da economicità, sovrapproduzione, e tendenza di stile, con effetti sull'ambiente devastanti[68]. Basti pensare alla circostanza che il settore è responsabile del 10% delle emissioni globali di gas serra[69].

12. Conclusioni.

Le istanze del Parlamento Europeo rendono evidente l'urgenza di una seria svolta nella politica consumeristica europea[70]. Il legislatore comunitario adotta

---

[65] In particolare sulla correlazione tra fast fashion, sostenibilità e responsabilità sociale, cfr. M. K. BREWER, *Slow Fashion in a Fast Fashion World: Promoting Sustainability and Responsibility*, in *The New Frontiers of Fashion Law,* a cura di R. E. CERCHIA, B. POZZO, Basilea, 2021, 47 ss.

[66] In particolare, l'obsolescenza nel settore della moda può ritenersi articolata su tre livelli: a) l'obsolescenza stilistica, l'obsolescenza fisica, obsolescenza da sovrapproduzione per approfondimento tematico cfr. M.F. TOMMASINI, *Fast fashion. Problemi giuridici*, in *Jus civile*, 2025, 2, 189.

[67] In tal senso è teorizzato il «*Manifesto della sostenibilità per la moda italiana*», promosso da Camera Nazionale della Moda Italiana (Milano, 13 Giugno 2012) che nelle linee guide sul design riporta: "1.Design. Disegna prodotti di qualità che possano durare a lungo e minimizzino gli impatti sugli ecosistemi: -Progetta prodotti di qualità che durino nel tempo".

[68] Nel 2020, il settore tessile è stato la terza fonte di degrado delle risorse idriche e dell'uso del suolo. In quell'anno sono stati necessari in media nove metri cubi di acqua, 400 metri quadrati di terreno e 391 chilogrammi di materie prime per fornire abiti e scarpe per ogni cittadino dell'UE. Fonte agenzia europea dell'ambiente (AEA)2023. Per quanto riguarda più specificamente i prodotti di abbigliamento, è stata distinta l'obsolescenza psicologica in estetica e sociale. Infatti tutto ciò che è correlato alla nostra apparenza e alla costruzione di sé stessi è valutato sia esteticamente sia socialmente. Esteticamente perché gli oggetti di moda intrinsecamente comportano uno stile, un aspetto, una forma, un colore che sono aspetti transitori e molto spesso legati ad una FAD, una moda transitoria. Il problema su cui riflettere e su cui agire è la dismissione di un prodotto pienamente funzionante, esclusivamente per il suo aspetto estetico, in questi termini cfr. B.B. BURNS, *Re-evaluating Obsolescence and Planning for It*, in *Longer Lasting Products: Alternatives to the Throwaway Society*, a cura di T. COOPER, Farnham, 2013, 39-60.

[69] Fonte agenzia europea dell'ambiente (AEA)2023 Gli acquisti di prodotti tessili nell'UE nel 2020 hanno generato circa 270 kg di CO_2 per persona. Questo significa che i prodotti tessili consumati nell'UE hanno generato emissioni di gas serra pari a 121 milioni di tonnellate. In tal senso cfr. S.S. MUTHU, *Roadmap to Sustainable Textiles and Clothing: Environmental and Social Aspects of Textiles and Clothing Supply Chain*, Singapore, 2014 citato in Greenpeace, *Timeout for fast-fashion.*

[70] In termini comportamentali viene coniata una nuova tipologia di consumatore il "LOHAS" ovvero Lifestyles of Health and Sustainability: è un tipo di consumatore che persegue, nelle scelte quotidiane, uno stile di vita basato sull' ecosostenibilità.Questo tipo di consumatori sceglieranno prodotti biologici a filiera corta, case con certificazione di classe energetica A, prediligeranno spostamenti puliti e, se costretti ad usare l'auto, sceglieranno quella con una maggiore efficienza energetica e con ridotte emissioni. Quello che distingue i

una strategia legislativa capillare, intervenendo nella fase genetica della formazione del consenso del consumatore che deve sempre essere pienamente informato e non fuorviato da pratiche commerciali ingannevoli. L'effetto sul mercato è conseguente all'intervento sugli attori del mercato. Il consumatore [71] diviene soggetto proattivo e interprete del cambiamento attraverso la realizzazione di una funzione sociale informata alla reale ed effettiva sostenibilità con attributi di circolarità economica [72], non solo apparente, ma sostanziale [73]. In questi termini la direttiva di contrasto al greenwashing e all'obsolescenza programmata, se recepite tempestivamente, fedelmente e in modo omogeneo da tutti Stati membri potrà sortire ricadute rilevanti sia in termini di rafforzamento amministrativo della vigilanza sul mercato, attraverso la giurisdizione amministrativa ordinaria e l'autorità garante della concorrenza e del mercato, sia sul piano dell'efficacia del sistema di avvisi armonizzati ed etichette armonizzate che attestino le qualità effettive dei prodotti anche in termini di eccellenza. L'AGCM, nel provvedimento n. 31135 del 12/03/2024 non ha perso occasione di definire come scorrette o aggressive quelle pratiche di vendita che compromettono i diritti del consumatore nella fase post-vendita, con particolare riferimento alla consegna, all'assistenza post-vendita, alla mancata conformità del prodotto e alle garanzie di durata. Tutte opzioni queste ultime che conferiscono rilevanza ai concetti di circolarità, durabilità e riparabilità del prodotto, di per sé idonee a

LOHAS dai classici consumatori "eco" è che oltre ad essere attenti all'ambiente, rispettosi e coscienti della salute e della società, non vogliono rinunciare alla moda e alla tecnologia, vivono nelle aree urbane, e vogliono essere coinvolti nella progettazione dei prodotti, cfr. S. SAVIOLO, S. TESTA, *Le imprese del sistema moda, il management al servizio della creatività*, Milano, 2013, cap. 1.2.

[71] Prime ricostruzioni teoriche innovative sulla funzione che deve svolgere il consumatore, nel senso di pretendere trasparenza, confronto e assunzione di responsabilità sociale per il rispetto dell'ambiente in un rapporto che non si esaurisce più quindi con acquisto e consumo, così da arrivare a parlare di "Consum-autore" in G. FABRIS, *Il nuovo consumatore: verso il postmodermo,* 2003, Milano, 94.

[72] Con riferimento alle interazioni tra giuridiche tra il concetto di sostenibilità e quello di transizione ecologica, cfr. A. MOLITERNI, *Transizione ecologica, ordine economico e sistema amministrativo*, in *Riv. dir. comp.,* 2022, 149 ss.; N. BASIGNI, C. PIFFER, D. PORENA, *Nuove prospettive di sostenibilità intergenerazionale: la sostenibilità delle materie prime nella transizione tecnologica energetica,* in *ambientediritto.it*, 2022, 149 ss.; B.L. BOSCHETTI, *Oltre l'art. 9 della Costituzione: un diritto (resiliente) per la transizione (ecologica),* in *DPCE online*, 2022, 1153 ss.; F. CUSANO, *L'efficienza energetica nel quadro della transizione ecologica,* in *Riv. quadr. dir. amb.*, 2022, 150 ss.; A.G. ANNUNZIATA, *Transizione ecologica e funzione della responsabilità civile,* in *Contr. impr. Eur.*, 2022, 391 ss.; A. ZAGARELLA, *La transizione ecologica nel PNRR tra 'climate change' e 'do not harm',* in *DPERonline,* 2022, 71 ss. Invece, per una compiuta analisi nel settore agroalimentare, si rinvia a S. MASINI, "*Transizione ecologica" dell'agricoltura*, in *Dir. agroal.,* 2022, 45 ss.

[73] All'art. 23, il d.lgs. 30/2026 prevede l'inserimento di nuove fattispecie «per se» vietate, tra cui (i) esibire una etichetta di sostenibilità non basata su sistema di certificazione o non stabilita da generiche senza poter dimostrare l'«eccellenza riconosciuta» pertinente alle asserzioni medesime; (iii) proporre claims ambientali «complessivi» su prodotto/attività quando riguardino però solo un aspetto specific dello stesso; (iv) asserire impatti neutri, ridotti o autorità pubbliche; (ii) formulare asserzioni ambientali positivi in termini di gas serra sulla base della compensazione delle emissioni. Tra i primi commentatori cfr. A. LETIZI, *Greenwashing: Strategie di contrasto e tutele civili nel nuovo Codice del Consumo dopo il D.Lgs. n. 30/2026*. Milano, 2026; AA.VV, *La responsabilizzazione del consumatore per la transizione verde. Commentario al D.Lgs. 20 febbraio 2026, n. 30*, a cura di G. RECINTO, S. PAGLIANTINI, Napoli, 2026; G. DE CRISTOFARO, *La nuova 'black list' delle pratiche commerciali ingannevoli: riflessioni critiche sull'attuazione della Direttiva (UE) 2024/825*, in *Le Nuove Leggi Civili Commentate*, 2026, 3, 412-435, E. MINERVINI, *I 'green claims' alla prova del mercato: profili rimediali dopo la novella del marzo 2026*, in *Diritto dell'Economia*, 1, vol. 72, 89-114. Nello specifico Esamina il coordinamento sistematico tra l'art. 23 D.Lgs. 30/2026 e il futuro quadro normativo europeo sulle asserzioni ambientali esplicite U. RUFFOLO, *Il recepimento della direttiva anti-greenwashing e l'ampliamento degli obblighi informativi: verso la Direttiva Green Claims*, in *Il Diritto degli Affari, Focus Impresa & Ambiente*, 2026, 1; A. BONAFINE, *Il decreto attuativo della Direttiva contro il greenwashing e i possibili riflessi sul contenzioso futuro. Note a prima lettura*, in *Judicium,* 15.04.2026.

spostare l'attenzione del consumatore anche sulla fase della vita del prodotto successiva alla vendita [74]. In conclusione, una strategia coerente a livello europeo è in atto, un ruolo fondamentale per il successo della pianificazione comunitaria sarà rappresentato dal fedele recepimento della direttiva in tutti gli Stati membri e dalla consapevolezza negli atti di vendita e di acquisto di produttori e consumatori destinatari delle disposizioni.

[74]Cfr. S. BADEN, C. BARBER, *The impact of the second-hand clothing trade on developing countries*, 2005, Oxfam, 12.

Di Gregorio V, 'Artificial Intelligence in the EU Digital Market: Data circulation and fundamental rights protection' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252VDG

EJPLT
ISSN 2704-8012



Artificial Intelligence in the EU Digital Market: Data circulation and fundamental rights protection

Intelligenza artificiale nel mercato digitale dell'UE: circolazione dei dati e tutela dei diritti fondamentali

VALENTINA DI GREGORIO
Associate Professor of Private Law
University of Genova

Abstract

This article offers an in-depth analysis of the recent European regulatory framework governing artificial intelligence and data circulation, with particular regard to the structural tension between the objective of fostering economic growth within the digital single market and the imperative of safeguarding fundamental rights. Tracing the evolution of the European Union's normative approach (from the initial emphasis on data protection, as enshrined in the General Data Protection Regulation (GDPR), to the emergence of a 'Data Economy' paradigm, embodied in the Data Governance Act and the Data Act) the study concentrates on the AI Act and its application in the digital regulatory context.

Questo articolo offre un'analisi approfondita del recente quadro normativo europeo che disciplina l'intelligenza artificiale e la circolazione dei dati, con particolare attenzione alla tensione strutturale tra l'obiettivo di promuovere la crescita economica all'interno del mercato unico digitale e l'imperativo di tutelare i diritti fondamentali. Ripercorrendo l'evoluzione dell'approccio normativo dell'Unione Europea (dall'iniziale enfasi sulla protezione dei dati, sancita dal Regolamento generale sulla protezione dei dati (GDPR), all'emergere di un paradigma di "economia dei dati", incarnato dal Data Governance Act e dal Data Act) lo studio si concentra sull'AI Act e sulla sua applicazione nel contesto normativo digitale.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Artificial Intelligence; European AI Act; Data Circulation; Digital Market, Civil Liability; Product Liability; Fundamental Rights

Summary: 1. Introduction: Recent European Legislative Initiatives in the Digital Sector. – 2. The Circulation of Data: from Data Protection to Data Economy. – 3. The AI Act within the Framework of the EU Single Market for Data. – 4. Conclusion: Regulatory Perspectives on Liability in the field of AI.

1. Introduction: Recent European Legislative Initiatives in the Digital Sector.

The transformation of the technological landscape has been driven by scientific and technological advances that have unfolded since the beginning of the new millennium.[1]

Central to this transformation are the emergence of digital and computational science, robotics, and bioengineering–fields grounded in algorithms and machine learning methods that can be broadly framed under the concept of Artificial Intelligence. These developments have enabled the creation of increasingly sophisticated algorithms and statistical models capable of self-learning and autonomous decision-making, replicating human processes of reasoning and interpretation, and exploiting the vast amounts of data available in the Information and Communication Technology (ICT) market.[2]

From the Alan Turing machine to driverless cars, drones, medical robotics, and the Internet of Things, the phenomenon of human–machine interaction has become central to both scientific and philosophical inquiry.[3]

The areas of reflection extend beyond issues of system safety and reliability to include ethical considerations understood both as a set of principles for the design and development of new technologies, and as a body of rules concerning the behaviour of machines and artificial intelligence. These considerations arise within scientific disciplines that foster human interconnectivity and, over time, reshape the ways in which social and commercial relationships are created and conducted.[4]

---

[1] According to Y Qian, KL Siau, FF Nah, 'Societal impacts of artificial intelligence: Ethical, legal, and governance issues' (2024) Societal Impacts 3, art. 100040 "Artificial intelligence (AI) is quickly changing the way we work and the way we live. The emergence of ChatGPT has thrust AI, especially Generative AI, into the spotlight. The societal impact of AI is on most people's minds".

[2] See M Jirotka, BC Stahl, 'The need for responsible technology, Journal of Responsible Technology' (2020) 1, art. 100002 according to whom "Tools and technologies are not objective, neutral and external facts for humans, but they shape our outlook on the world, our capability to act, the very nature of our society".

[3] Among the Italian legal literature, see inter alia: G Finocchiaro, *Diritto dell'intelligenza artificiale* (2024); U Ruffolo (ed.), *Intelligenza artificiale: il diritto, i diritti, l'etica* (2020); G Alpa, *L'intelligenza artificiale. Contesto giuridico* (Mucchi 2021); G Alpa (ed.), *Diritto e intelligenza artificiale* (Pacini 2020). Forward-looking insights on the current debate were already present in: S Rodotà, *Tecnologie e diritti* (Il Mulino 1995); N Lipari, *Le categorie del diritto civile* (Giuffrè 2013). For comparative perspectives, see: E Lim and P Morgan, *The Cambridge Handbook of Private Law and Artificial Intelligence* (Cambridge University Press 2024); A Häuselmann, 'Disciplines of AI: An Overview of Approaches and Techniques' in B Custers and E Fosch-Villaronga (eds), *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice* (TMC Asser Press 2022) 43; M Ebers and S Navas, *Algorithms and Law* (Cambridge University Press 2020).

[4] L Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide* (Pacini 2022) 145; R Basili, 'Sistemi intelligenti e dati: opportunità e rischi etici', in A Morace Pinelli, *La circolazione dei dati personali. Persona, contratto e mercato* (Pacini 2023) 121. On the topic, see also the European Parliament Resolution of 20

The vast availability of circulating data – undeniably a driving force for the economy and a catalyst for rapid technological innovation that has accelerated the digitalisation of products and services – has prompted the European legislator to intervene by establishing a regulatory framework aimed at maintaining oversight over the safety and reliability of AI systems, while also enhancing the competitiveness of European businesses and fostering cooperation among Member States.[5]

In the area of artificial intelligence, the recent Regulation (EU) 2024/1689, known as the AI Act, has introduced a regulatory framework designed to promote innovation while safeguarding fundamental rights such as liberty, privacy, security, health, environmental protection, democracy, and the rule of law, as enshrined in the Charter of Fundamental Rights of the European Union.[6]

The European legislator has progressively shifted its approach – from a predominant focus on data protection, as established by Regulation (EU) 2016/679 (GDPR) for personal data and Regulation (EU) 2018/1807[7] for non-personal data, to the growing emphasis on the value of interoperable data (both personal and non-personal) within a broader data-sharing framework. This shift reflects the strategic aim of achieving Europe's 'technological sovereignty,' a central objective of Regulation (EU) 2022/868 (the Data Governance Act, DGA) and Regulation (EU) 2023/2854 (the Data Act, DA), both of which form integral parts of the EU's regulatory architecture on data governance.

This evolution reflects a fundamental dialectic within the EU legal order, which seeks to balance the protection of the individual, with data protection enshrined as a fundamental right, against the imperative to promote market development through the free circulation of data. Historically, the focus on personal data and its link to the protection of the person hindered the notion of a market for personal data, subject not only to the rules guaranteeing individual rights but also to those governing business activity.[8] However, the undeniable economic utility of data has led the European and national legislators in recent years to maximize the economic exploitation of data, now recognized as negotiable assets that circulate through contractual instruments, fostering market development. The Data Governance Act (DGA)

October 2020 on the ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)) (P9_TA (2020)0275), and the Ethics Guidelines for Trustworthy AI published by the European Commission's High-Level Expert Group on AI in 2019.

[5] As set out by the European Commission in its 2020 European Data Strategy, which aimed to strengthen European competitiveness through the establishment of a "European single data space". On the challenges faced by regulators in the data economy, specifically from the perspective of AI, see: M Nitzberg and J Zysman, 'Algorithms, Data, and Platforms: The Diverse Challenges of Governing AI' (2022) Journal of European Public Policy 1753.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L, art 3(2) defines an AI system as 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'. On this topic see R Rodrigues, 'Legal and human rights issues of AI: Gaps, challenges and vulnerabilities' (2020) Journal of Responsible Technology 4 art. 100005.

[7] European Commission, European Data Strategy (2020) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en>.

[8] A Morace Pinelli, 'Data Act (reg. UE 2023/2854): la circolazione dei dati nell'interesse privato e generale' (2025) Nuova giur. civ. comm. 218.

and the Data Act (DA) are expressions of this legal repositioning, aiming to revitalize the European data market while ensuring that data is Findable, Accessible, Interoperable, and Reusable (FAIR).[9] This regulatory strategy is not about replacing the GDPR but about creating a complementary framework where data can be shared and reused safely, including for altruistic purposes in the public interest, thus revealing the social function of data processing.[10]

The concern for maintaining a balance between technological development and the protection of fundamental rights is also reflected in the Framework Convention adopted by the Council of Europe in 2024 (n.225) on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. This Convention reaffirms the importance of ensuring that AI systems are grounded in principles of transparency, trustworthiness, and innovation, with particular emphasis on accountability, privacy protection, and democratic values.

Among other initiatives aimed at fostering sustainable growth and strengthening the EU's position in the digital and ICT markets is the 2022 Digital Services Package. In the financial sector, a notable ongoing legislative proposal is the Regulation on Financial Data Access (FIDA), presented on 28 June 2023 (COM (2023) 360 final). Within the framework of an Open Finance system, the proposed regulation seeks to 'improve financial outcomes for financial services customers (consumers and businesses) and for financial sector firms by promoting digital transformation and accelerating the adoption of data-driven business models in the financial sector'.[11]

Recently, on 19 November 2025, the European Commission presented the Digital Omnibus proposal, a landmark regulatory initiative designed to update and harmonize the European legal framework on personal data protection, cybersecurity and artificial intelligence. This proposal is part of the broader 'Implementation and Simplification Programme 2025,' which aims to reduce regulatory complexity and improve the consistency and accessibility of European Union law. For the digital finance ecosystem, the Digital Omnibus represents a critical step towards aligning the GDPR with the AI Act, NIS2, the Data Act, the DGA and the ePrivacy Directive, thereby fostering a more integrated and predictable environment for data-driven innovation.

The Digital Omnibus explicitly aims to strengthen consistency between these legal instruments, simplify certain compliance obligations for data controllers, and adapt the legal framework to the technological reality marked

[9] S Geiregat, 'The Data Act: Start of a New Era of Data Ownership?' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4214704>.

[10] A Hervé, 'Data Protection and Artificial Intelligence. The European Union's Internal Approach and Its Promotion through Trade Agreements', in T Streinz, S Peng, C-F Lin, Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration (Cambridge University press 2021) 193.

[11] P Stanzione, 'Open Banking, Open Finance and the Protection of Personal Data', in M Falace and S Morera (eds), Dall'Open Banking all'Open Finance. Profili di diritto dell'economia (Giappichelli 2024) 65; A Pajno, F Donati and A Perrucci, 'Intelligenza artificiale e diritto: una rivoluzione?', *Proprietà intellettuale, società e finanza* (Il Mulino 2022) 3. The Digital Services Package includes the Digital Services Act (Regulation (EU) 2022/2065, DSA), concerning the development of the digital economy in the field of networks and services, and the Digital Markets Act (Regulation (EU) 2022/1925, DMA), which addresses online platforms and competition. Other relevant instruments include Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market, Directive (EU) 2019/770 on contracts for the supply of digital content and digital services, and Directive (EU) 2019/771 on the sale of goods incorporating or interconnecting digital content or digital services. These instruments have contributed to integrating consumer protection rules in the digital technology sector, particularly in the context of data use in digital services.

by the widespread use of AI systems and the growing economic value of data. A key aspect is the introduction of greater flexibility in the timeline for compliance with high-risk AI system requirements, linking their applicability to the actual availability of technical standards and support tools. Another profile is the shift of the definition of personal data (Article 4(1) GDPR) from an objective standard of identifiability to a contextual and relative one. Under the new approach, data qualifies as 'personal' based on the reasonable means available to the data controller to identify an individual, rather than on a purely abstract possibility. This means that the same dataset may be considered personal data for a large financial institution with advanced re-identification capabilities, but not for a smaller FinTech firm lacking such technical means.[12]

The extensive regulatory framework (deemed necessary to ensure both the economic development of European businesses and the protection of fundamental right) has nonetheless raised questions regarding the compatibility between newly introduced sectoral rules and the general legal categories in force in individual Member States. This tension is particularly evident in areas such as the redefinition of the legal nature of personal data, the contractual requirements governing the use of network-connected and related products (as well as the validity of the clauses contained therein), and the criteria for assigning civil liability for damages caused by artificial intelligence systems: issues that are currently the subject of ongoing academic debate.[13]

Such a tension reflects a deeper constitutional challenge. The emergence of large digital platforms as private powers, often in competition with public authorities, has necessitated a rethinking of constitutional tools. The goal is to contain this new, horizontally exercised power while remaining faithful to constitutionalism's core mission of limiting power and protecting fundamental rights, a process that can be framed as the rise of 'digital constitutionalism'.[14]

This concept denotes a rethinking of constitutional tools to contain the new, horizontally exercised private power of large digital platforms, remaining faithful to constitutionalism's core mission of limiting power and protecting fundamental rights. In the context of AI regulation, this translates into an effort to establish ex-ante, horizontally applicable rules, representing a reappropriation by the political-representative circuit of its role as law-maker, moving beyond the ex-post enforcement and sectoral fragmentation that characterized the earlier, more court-driven phase of the European response.[15]

---

[12] Proposal 19.11.2025 COM(2025) 837 final 2025/0360(COD) for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), accessible at <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>.

[13] The most recent version of the proposal for a directive of the European Parliament and of the Council is dated 28 September 2022 and is available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>.

[14] O Pollicino, *Costituzionalismo digitale. Pensare la democrazia al tempo dell'AI* (Bologna 2025); ibid 'Di cosa parliamo quando parliamo di costituzionalismo digitale?' (2023) Quad. cost. 569.

[15] A Simoncini, 'La dimensione costituzionale della giustizia predittiva. Riflessioni su intelligenza artificiale e processo' (2024) Riv. dir. proc. 405.

The European regulatory impetus has spurred, in turn, a series of national legislative initiatives aimed at disciplining and promoting the responsible use of AI across Member States.

A prime example is the recent Italian Law No. 132 of 23 September 2025 (Provisions and Delegations to the Government on Artificial Intelligence).[16] The new Law explicitly aims to promote a correct, transparent, and responsible use of AI, anchored in an anthropocentric dimension (Art. 1, co. 1), and, critically, establishes that its provisions shall be interpreted and applied in conformity with the Regulation (EU) 2024/1689 (AI Act) (Art. 1, co. 2). As outlined above, it demonstrates the crucial role of national law in establishing a coordinated domestic governance structure within the primary framework of EU harmonization.

This regulatory shift towards a risk-based, ex-ante logic, however, brings to the fore a fundamental tension with traditional civil liability frameworks. The preventive logic of the AI Act, centred on conformity assessment and the classification of systems, does not seamlessly address the ex-post question of who should bear the cost of harm when a 'conformant' system, particularly a highly autonomous one, causes damage. This consideration is particularly relevant in high-stakes sectors like healthcare, where the use of autonomous AI systems creates a potential 'liability gap', as the unpredictability of the system's autonomous decisions may sever the chain of imputation from the human user, who can no longer be reasonably expected to foresee or control its actions.[17]

2. The Circulation of Data: From Data Protection to Data Economy.

Since data circulation is both a key driver of the economy and increasingly powered by artificial intelligence, the European legislator adopted the Data Governance Act in 2022. This regulation, dedicated to the governance of European data spaces, embraces a transformative and dynamic vision of the digital economy. It aims to revitalise the European data market (encompassing both personal and non-personal data) while ensuring FAIR access: Findable, Accessible, Interoperable, and Reusable. Although technological innovation and data protection are also central to the General Data Protection Regulation (as highlighted in Recitals 2, 6, and 9), the Data Governance Act seeks to enhance its effectiveness by unlocking vast volumes of data for economic development. It ensures their safe and free circulation through provisions on the re-use of public sector data, data intermediation services, and the voluntary registration of entities collecting and processing data for altruistic purposes.

This regulatory strategy is structured around four foundational pillars, the first of which sets out an ‘integrated’ legal framework aimed at improving access to data and promoting more responsible and innovation-friendly data

[16] Law No. 132 of 23 September 2025, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, published in G.U. n. 223 of 25-9-2025, Art. 1, co. 2.

[17] See A D’Adda, ‘Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo’ (2022) Riv. dir. civ. 807, who highlights the core problem that the autonomy of a machine is not neutral for liability and can create a gap, particularly for the user, due to the uncontrollability of the robot's anomalous manifestations.

practices. This approach is further developed in the subsequent Data Act, which seeks to enhance access for consumers and businesses to data generated, in particular, by Internet of Things devices.[18]

The remaining pillars support EU's action by promoting the creation of common European data spaces and interconnected cloud infrastructures to overcome legal and technical barriers to data sharing across Europe (second pillar); by enhancing individual empowerment through support measures for the use of data generated by digital devices and by creating better opportunities within the data economy for legal persons (third pillar); and by strengthening the role of public sector bodies and promoting the development of common European data spaces in strategic economic sectors and other areas of public interest (fourth pillar).

This approach is also reflected, beyond the explicit references found in the legislation, in the terminology adopted by the regulatory texts themselves. The notion of 'data holder' (as opposed to 'data controller') refers to the entity that 'has the right or obligation to use and make data available' (Article 2(13) of the Data Act) and is subject to specific rights and obligations.

Accordingly, data is no longer seen solely as an object of protection but also as a legal asset with economic potential to be exploited fairly and transparently within the limits imposed by the need to prevent misuse that could infringe fundamental rights. These risks may be amplified by data-driven practices and the increasing use of artificial intelligence.

The regulation offers companies the opportunity to optimise production processes and improve services related to the manufacturing of technological devices and industrial machinery. It enables the exploitation of AI-based resources through connected devices (such as IoT products, drones, smart cars, healthcare devices, and virtual assistants) and associated product-related services, often provided along with cloud-based solutions. This framework fosters innovation and competition, while ensuring respect for trade secrets, anti-discrimination rules, [19] and safeguards against contractual power asymmetries between parties.[20]

In this context, data-driven or data-based artificial intelligence systems, which collect, analyse, and process data through algorithms capable of extracting information that enriches the market of digital companies,

[18] D Poletti, 'Gli intermediari dei dati' (2022) EJPLT 46; G Krutzinna and L Floridi, 'Ethical Medical Data Donation: A Pressing Issue' in G Krutzinna and L Floridi (eds), *The Ethics of Medical Data Donation* (Springer 2019); E Curry, S Scerri and S Tuikka, *Data Spaces. Design, Deployment, and Future Directions* (Springer 2022) <https://doi.org/10.1007/978-3-030-98636-0_1>.

[19] Regulation (EU) 2023/2854 distinguishes between obligations imposed on manufacturers of connected products placed on the European market and those applicable to providers of data processing services, including cloud services. It lays down harmonised rules aimed at removing barriers to data sharing and ensuring that data generated by a connected product – defined as 'an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access' (article 2(5)) – and by a related service – defined as 'a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase or afterwards and which affects the functioning of the product or the services provided by it' (article 2(6)) – shall be 'easily, securely, free of charge, and, where relevant and technically feasible, directly accessible to the user in a comprehensive, structured, commonly used and machine-readable format' (article 3(1)).

[20] From this perspective, the Data Act includes provisions that partially overlap with those set out in the Italian Consumer Code (Legislative Decree No 205/2006, art 33), which prohibits clauses that unilaterally impose conditions limiting access to or use of data between businesses.

contribute to wealth generation by enabling the provision of higher-quality or more tailored products and services for users, whether individuals or businesses.[21]

3. The AI Act within the Framework of the EU Single Market for Data.

Within the digital market framework, the AI Act regulates a rapidly growing sector with great and unpredictable potential, through a structured body of provisions concerning the classification of AI systems, the procedures for assessing compliance with the prescribed requirements, and the organization of supervisory and control bodies.

Given that artificial intelligence is data-driven, it is appropriate to reflect on the relationship between the widespread dissemination of the phenomenon (now easily accessible across society) and its regulation in the most recent EU legal acts.

From an initial stance of distrust towards the potential of information technology – due to the risk it posed to personal rights and security – the EU has gradually recognized the market opportunities offered by these technologies. The AI Act positions itself as a key component of a regulatory framework aimed at fostering market development. It adopts an industrial policy approach, based on the risk-based model (Article 3(2) defines risk as a 'combination of the probability of occurrence of harm and the severity of that harm') and product safety, already outlined in the 2021 proposal.

This risk-based, industrial policy approach embodies a shift from a purely jurisdictional reaction to a proactive, political-law-making effort to contain private digital power through horizontal rules. However, the constitutional challenges extend beyond the legislative framework to its application, particularly in sensitive areas like the judiciary. The use of AI, especially generative AI, in judicial decision-making – so-called 'predictive justice' – raises profound constitutional questions regarding the right to a transparent and understandable decision, the judge's impartiality, and the very freedom of the judge to be subject only to the law, free from the deterministic prescriptiveness of algorithmic outputs based on past data.[22]

In promoting a human-centric and trustworthy AI (Article 1), the regulation sets out differentiated obligations according to the level of risk posed by each category of system, in relation to potential infringements of individuals' rights and freedoms. This logic encourages the development and use of AI (even high-risk AI) to support entrepreneurship and investment in the sector. It also imposes obligations on non-EU companies (Article 2) to comply with the Regulation and related harmonized standards, while pursuing a different rationale than the GDPR, which primarily seeks to protect personal data from unlawful access and processing.

Aside from the prohibited AI practices listed in Article 5 (deemed to pose unacceptable risks to safety, health, or fundamental rights) the Regulation

[21] See S. Wachter, B. Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Colum. Bus. L. Rev. 494.
[22] A Simoncini, 'La dimensione costituzionale della giustizia predittiva' (n 14) 415-416.

establishes a graduated risk scale ranging from high to minimal risk. For high-risk systems, enhanced oversight mechanisms are foreseen, including mandatory assessments to ensure compliance, and a consistent focus on fundamental rights. These systems are listed according to a typological approach in Annex I (referring to Union harmonization legislation) and Annex III, with potential extensions authorized by the Commission under Article 7.[23]

Low-risk systems are subject to specific transparency and information obligations (Article 50). These include systems interacting with natural persons, which must be designed to provide clear information about such interactions. When the output includes audio, images, video (including deepfakes), or text generated through data use, the system must clearly mark content in a machine-readable format, ensuring it is detectable as artificially generated or manipulated through effective, interoperable, robust, and reliable technical solutions. In the case of emotion recognition or biometric categorization systems, these obligations apply alongside compliance with the GDPR.

Additional provisions concern risk assessment procedures, such as the Fundamental Rights Impact Assessment (FRIA) under Article 27, and Conformity Assessment under Article 43, which may require the application of harmonized standards (Article 40). These assessments are aimed at identifying the risk level and ensuring regulatory compliance, with sanctions and liability for non-compliance, including non-contractual liability for damage caused by system failures.

For high-risk AI systems, Article 10 (Data and data governance) applies to all data types – personal and non-personal – governed by the GDPR and the Data Act. It mandates the implementation of processes for training, validation, and testing of datasets to determine data origin (and purpose, in the case of personal data), collection processes, updates, adequacy, treatment operations, representativeness, quantity and quality of data, and the presence of bias, gaps, or discriminatory elements that could undermine system reliability and safety. This is essential to prevent the violation of the foundational principles of the recent EU regulatory framework.[24]

The relationship between the AI Act, the Data Act, and the GDPR is therefore one of complementarity and hierarchy. Both the DGA and the Data Act explicitly affirm the primacy of the GDPR in case of conflict. This establishes a clear legal hierarchy: the foundational principles of data protection cannot be eroded by the newer regulations designed to foster the data economy. The AI Act, while operating within the single market framework and adopting an industrial policy approach, confirms this primacy in its Article 2(7). Consequently, when data processing for AI system development involves

[23] The AI Act's focus on the governance of high-risk AI systems is reflected in the institutional choices of the Member States. To implement the Regulation effectively and ensure domestic supervision, the Italian Law No. 132/2025 establishes the National AI Agency (Art. 3), entrusted with supervisory and enforcement functions. This institutional structure is tasked with ensuring compliance, overseeing economic and social risks, and monitoring the impact of AI on fundamental rights, thereby complementing the AI Act's risk-based approach with a specific national enforcement mechanism.

[24] Regulatory recitals emphasize the principle of data reliability: the AI Act (recitals 1, 6), the Data Governance Act (recital 3), and the Data Act (recital 30) stipulate that 'data holders should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date as the data the data holder itself may be able or entitled to access from the use of the connected product or related service'.

personal data, particularly special categories of data, the GDPR provides the legal basis and the core protections.

The Data Act further refines this interaction in the context of data generated by connected products. It mandates that data holders must make data available to users and third parties, but if the user is not the data subject, personal data can only be shared if there is a valid legal basis under Article 6 GDPR. This creates a complex interplay where contractual tools for data sharing, promoted by the Data Act, must operate within the inviolable limits set by the GDPR to protect fundamental rights, with the data subject's dignity acting as the ultimate, insurmountable limit to data circulation in the market.[25]

Algorithmic decision-making processes can lead to unintentional biases, especially in critical sectors like healthcare or credit scoring.

When such bias assessments require processing personal data – particularly special categories of data (Article 7(2)(c)) – the AI Act confirms the primacy of the GDPR (Article 2(7)). Article 10(5) introduces specific data protection and security obligations to prevent abuse, unauthorized access or transfers, and mandates deletion of data once the necessary processing is completed.

These rules also apply to General-Purpose AI (GPAI) models, also known as generative AI, which create new content using information collected online (including user-generated data).[26] These tools have raised concern – reflected in decisions by Italy's data protection authority – due to uncertainties regarding compliance with the above requirements and the risk of losing control over (even personal) data.

To address this, Article 53 (Obligations for providers of GPAI models) imposes additional requirements, including documentation on model characteristics and its training, validation, and testing processes. It establishes obligations on accountability, transparency, and information for providers integrating such models and mandates a public register of GPAI models with systemic risk (Article 52), as well as compliance with copyright and data protection law. Exceptions apply to open-source models, where parameters must be made public.

For GPAI models with high-impact capabilities, Article 51 introduces the category of systemic risk, based also on quantitative thresholds (Article 51(2)). These are subject to enhanced conformity assessments, including standardized protocols, risk monitoring, incident logging, cybersecurity guarantees, and the drafting of Codes of Practice (Article 51).

Algorithms, data, computing power, and digital platforms (understood both as societal actors and technological infrastructure) generate the Big Data pools used by AI systems. They form the interface between data regulations and the AI Act, [27] which together reflect the EU's strategic vision for the digital society: a trajectory that began with ICT and internet development, advanced through the data economy, and has now culminated, after multiple ethical and legal

[25] On this topic see C Pinelli, 'L'AI Act: gestione del rischio e tutela dei diritti' (2025) Giur. it. 452.

[26] On the applications of generative AI, see, among others, I Botunac et al, Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA, presented at the 13th Mediterranean Conference on Embedded Computing (MECO), 11–14 June 2024, Budva, Montenegro.

[27] On the relationship between the Data Act and other European legal instruments, see, among others, A Fernandez, 'The Data Act: The Next Step in Moving Forward to a European Data Space' (2022) Eur. Data Prot. Law Rev. 108, especially 111.

resolutions on AI, in a broad regulatory framework with the goal of positioning Europe as a global AI leader (Article 1, AI Act).

4. Conclusion: Regulatory Perspectives on Liability in the field of AI.

It has already been observed that within the considerable number of legislative acts issued by the EU and spread across various digital law texts, there is a lack of focus on the consequences of AI use in terms of civil liability. A liability regime in this area should aim to protect those harmed without stifling scientific and technological innovation or economic development.[28]

Currently, liability for damages arising from the use of AI – such as an algorithm's error used to produce a result (for example, in the healthcare field, where human oversight remains a fundamental principle), the malfunctioning of a connected product or related service due to a defect in the algorithm's design or development, the unlawful extraction of data through an application, or the absence of requirements mandated by regulatory law – is left to the legislation of each individual country. The lack of a harmonized framework reveals the EU's difficulty in establishing a general system capable of regulating the consequences of technological and scientific advancements in a way that aligns with national liability rules across Member States.

From this perspective, the recent Product Liability Directive (EU) 2024/2853, which replaces the previous directive transposed into the Italian Consumer Code, does not establish a specific non-contractual liability regime for AI. However, it clearly aims to set rules for digital products and services, inspired by principles shared among various legislative acts related to the digital market. This intention is confirmed in the definitions section, which now includes products of the modern digital and circular economy. A product is defined as 'all movables, even if integrated into, or inter-connected with, another movable or an immovable; it includes electricity, digital manufacturing files, raw materials and software' (Article 4(1)).[29]

This modernized definition explicitly encompasses software and digital manufacturing files, thereby extending the directive's scope to AI-based platforms and robots with integrated AI. Crucially, Article 7(2)(c) now mandates that the assessment of a product's safety, and thus its potential defectiveness, must take into account "the effects on the product of its ability to continue to learn or acquire new functionalities after it has been placed on the market or put into service." This represents a significant step towards addressing the specific challenges posed by adaptive AI systems. Furthermore, to alleviate the claimant's burden of proof - a key weakness of the previous regime - the new directive introduces a right to disclosure of relevant evidence held by the defendant (Article 9) and establishes several rebuttable presumptions. For

[28] On this point, see also G Brüggemeier, *Tort Law in the European Union* (Kluwer Law International 2018); see also W Barfield and U Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar Publishing 2019).

[29] For a discussion on the rationale and implications of this broader definition, see G Ponzanelli, 'Responsabilità da prodotto difettoso: dalla Dir. n. 374 del 25 luglio 1985 alla nuova Dir. n. 2853 del 23 ottobre 2024' (2025) Danno resp., 153. See also, to the same effect, M Franzoni, 'Note sulla nuova direttiva sul danno da prodotti' (2025) Danno resp. 57.

instance, a defect can be presumed if the product does not comply with mandatory safety requirements, or if the damage was caused by an obvious malfunction during reasonably foreseeable use. A causal link between the defect and the damage is also presumed where the product is proven to be defective and the nature of the damage is consistent with that defect (Article 10).[30]

To facilitate the protection of users' and consumers' rights, the Directive allows injured parties to request access to relevant evidence held by the producer in order to substantiate their right to compensation (Article 9), introducing a system of presumed liability. The burden of proof follows a regime partly based on Article 120 of the Italian Consumer Code, requiring proof of the defectiveness of the product, the damage, and the causal link (Article 10(1)), without the need to prove the producer's fault. Additionally, a new rule presumes a causal link between defect and damage if the defective nature of the product and the nature of the resulting damage are consistent (Article 10(3)).[31] A further easing of the burden of proof for the injured party is provided in cases of particular technical or scientific complexity, where demonstrating either the probability that the product was defective or that the defect was likely the cause of the damage is sufficient (Article 10(4)), subject to contrary evidence by the producer (Article 11).

Similar evidentiary provisions appeared in the proposed directive on non-contractual liability for artificial intelligence, [32] which described a rather complex liability framework based on rebuttable presumptions to ease the burden of proof for injured parties and encourage compliance with diligence obligations established at the national or EU level. However, the proposal stopped short of fully reversing the burden of proof so as not to hinder innovation or the uptake of AI-based products and services. In particular, the draft included a presumption of a causal link between the defendant's fault and the AI system's output (or lack thereof) under specific circumstances. The same rationale underpinned rules related to high-risk AI systems, such as tools for identifying potentially liable parties and obtaining relevant evidence through court-ordered disclosure or preservation measures, while still safeguarding trade secrets and confidential information (Article 3). For high-risk systems, the latest version of the proposal laid out specific rules for providers (or those subject to the provider's obligations), linked to compliance with the conformity

[30] ibid 154–155.

[31] Art 9(3): The existence of a causal link between the defectiveness of the product and the damage is presumed where it has been proven that the product was defective and that the nature of the damage caused is generally consistent with the defect in question. This issue warrants further analysis, which cannot be undertaken here and is deferred to another work. See P Trimarchi, *Rischio e responsabilità oggettiva* (Giuffrè 1961). Among those in favour of considering the producer's liability as objective due to the absence of a fault-based imputation criterion are F Galgano, 'Responsabilità del produttore' (1986) Contr. impr. 995; G Visintini, *I fatti illeciti*, II, (Cedam 1990), 318; M Comporti, 'Fatti illeciti: le responsabilità oggettive', in P Schlesinger and FD Busnelli, *Commentario al codice civile* (Giuffrè 2009) 185. The thesis supporting the plurality of imputation criteria is upheld by C Salvi, 'La responsabilità civile', in G Iudica and P Zatti, *Trattato di diritto privato* (Giuffrè 2019) 3, 161.

[32] The proposal for a directive of the European Parliament and of the Council of 28 September 2022 on adapting non-contractual civil liability rules to artificial intelligence (Artificial Intelligence Liability Directive), COM/2022/496 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>, has since been withdrawn, partly due to widespread criticism of the liability framework it proposed, and currently shows no prospect of being adopted.

requirements set forth by the AI Act, based on the associated risk level. (For English terminology, refer to the official directive text.)

In 2020, the issue had already been addressed in the European Parliament's resolution on civil liability for artificial intelligence, and later in the original 2021 proposal for a Regulation on the harmonisation of AI rules [33] (later replaced by the 2024 AI Act). This resolution advocated for a strict liability regime based on risk, alongside mechanisms enabling the harmed party to identify the individual capable of controlling the AI system or verifying which code, input, or data caused the harm. Responsibility was attributed to both 'front-end operators' – natural or legal persons who deploy the AI system and benefit from its operation – and 'back-end operators,' such as the technology producer, developer, programmer, or service provider.

To adapt existing liability frameworks across jurisdictions, the proposal envisaged a dual liability regime: one strict liability regime for operators of devices or processes driven by high-risk AI systems (to be listed in a specific annex); and a fault-based regime for less risky systems, grounded in a presumption of fault in clearly defined cases and following adequate assessment. This would relieve the victim from proving the defect, even without evidence of an elevated risk compared to other products, while encouraging compliance with applicable conformity requirements.[34]

The 2024 AI Act, however, chose to outline a horizontal regulation for the use of AI without introducing a unified liability regime.

In the Italian legal system, when addressing damages from AI use, reference is generally made to Articles 2049, 2050, and 2051 of the Civil Code and to the rules on defective products within the Consumer Code.[35]

The application of these national provisions to AI-related harm is the subject of a significant doctrinal debate in Italy. A prevalent view considers the custodian's liability under Article 2051 of the Civil Code as a potential solution, given its objective nature, requiring the custodian to prove *casus fortuitus* to avoid liability.[36] This approach is predicated on treating the AI system as a 'thing' under the custodian's control.

This application is highly contested, particularly for autonomous systems in medicine.

---

[33] See European Parliament, Resolution of 20 October 2020 on a civil liability regime for artificial intelligence (2020/2014(INL)) [2020] P9_TA(2020)0276; and European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM(2021) 206 final, 21 April 2021.

[34] M Faccioli, 'La responsabilità civile per danni cagionati da sistemi di intelligenza artificiale nel prisma dell'onere della prova' (2024) Resp. civ. prev. 950.

[35] U Ruffolo, 'Intelligenza artificiale, machine learning e responsabilità da algoritmo' (2019) Giur. it. 1689 and A Santosuosso, *Diritto, scienza, nuove tecnologie* (Cedam 2016) 338, regarding the analogy with parental liability under Article 2048 of the Italian Civil Code and liability for acts of persons lacking capacity under Article 2047. The recent Italian draft enabling law on artificial intelligence (d.d.l. n. 1146/2024), approved by the Senate, aligns with the principles underpinning EU regulatory instruments and introduces sector-specific rules on the use of AI in healthcare and disability, employment, liberal professions, public administration, and judicial decision-making. The law is accompanied by a broader set of provisions concerning AI governance and promotion, including the establishment of an independent authority. However, it does not address civil liability. The subsequent legislative decree will be tasked with adapting national law to the European regulation, following guiding principles aimed at enhancing the population's technological competence and including specific rules on copyright protection and criminal law.

[36] C Scognamiglio, 'Responsabilità civile ed intelligenza artificiale: quali soluzioni per quali problemi?' (2023) Resp. civ. prev. 1087-1088.

A significant strand of civilistic thought argues that applying such objective liability to the user (e.g., a surgeon or a hospital) for the actions of an autonomous surgical robot is problematic. While this would ensure maximum protection for the victim, it is criticised as inequitable and potentially disincentivising. The core of the criticism lies in the fact that such liability is imposed on a user who, by definition, could not predict or control the machine's 'black-box' decisions. This effectively holds the user liable as a 'guarantor' for the technological risk, a role traditionally associated with the producer who places the product on the market, not the professional who utilises it.[37]

However, this framework is contested by scholars who argue that the traditional notion of a 'thing' in Article 2051, conceived as a static entity, is a 'distant entity' from the dynamic and adaptive nature of an AI system, whose core function is processing and autonomous elaboration.[38] An alternative and widely supported view advocates for the application of Article 2050 concerning liability for dangerous activities. This provision, often described as an 'intermediate' principle between fault and risk-based liability, imposes liability on whoever causes damage through activities dangerous by their nature or the means used, unless they prove having adopted all suitable measures to avoid the damage[39]. The objective dangerousness of an activity is assessed in light of scientific and technical evolution, and the use of autonomous systems capable of learning is increasingly considered to fall within this category.

This legal basis appears more adaptable than product liability rules, as it does not rely on the static concept of a 'defect' conceived at the time the product is placed on the market, which is ill-suited for systems whose behavior evolves through continuous learning, potentially exposing the producer to the development risk defense.[40]

Article 2049, which establishes strict vicarious liability, appears irrelevant in this context, as the human-machine relationship cannot be equated to that between an employer/superior and an employee/subordinate, especially considering that AI is meant to replace human intervention to minimize error.

The other two articles outline strict liability scenarios, where liability is attributed based on the dangerous nature of the activity (Article 2050) or the relationship with the ‘thing’ (Article 2051). In both cases, specific defences are allowed: proof of having taken all reasonable precautions (Article 2050), or an unforeseeable event (Article 2051), which applies even if no custodial duty was violated since liability arises from the dynamic nature of the thing.

[37] A D’Adda, ‘Danni «da robot»’ (n 16) 807-808, critically examines the solution of imposing objective liability on the user, noting that while it protects the victim, it may unjustly burden the healthcare professional and disincentivise the use of beneficial AI technologies, given the fundamental lack of control over an autonomous system's operations.

[38] On a wider perspective: M Costanza, ‘L’intelligenza Artificiale e gli stilemi della responsabilità civile’ (2019) Giur. it. 687.

[39] Among others: F Di Lella, *Le attività pericolose nel settore bio-medico. Spunti per una rilettura dell’art. 2050 c.c.* (Pacini 2020) 60.

[40] This is also pointed out by A Mantelero, ‘L’AI Act: la risposta del legislatore europeo alle sfide dell’intelligenza artificiale’ (2024) Accademia 197.

Article 2050, often described as an 'intermediate' principle between fault and risk-based liability [41] may not cover AI and robotics if they increase safety levels compared to human action, as is the case in medicine. However, it could be applied by assessing whether all appropriate measures were taken to avoid harm, thereby safeguarding safety and security across sectors without stifling beneficial technological progress.

The new Product Liability Directive also adopts a risk-based evaluation of products (including algorithmic errors) aiming to balance research initiatives, investment, market uptake of new technologies, and fundamental rights protection, such as health. Since the definition of 'product' (Article 4) now includes software, raw materials, and digital manufacturing files, this could extend to AI-based platforms and robots with integrated AI, unless covered by the Machinery Directive. However, digital content, multimedia files, ebooks, and software source code would be excluded, as governed by other relevant acts.

If AI software is considered a 'product' and if continuous learning is deemed analogous to updates or improvements (Articles 4 and 7 and Recital 40), the Directive could be applied.

While the Directive includes software-based products and possibly AI systems, it does not offer a comprehensive liability framework for AI, especially when the elements required for product liability – such as the product status of the AI system or damage types expressly listed in Article 6 (death, personal injury, or property damage) – are missing. The Directive is less applicable to damages affecting reputation, privacy, personality rights in general, or non-professional data loss, IP infringement, and discriminatory harm: this last being particularly relevant given the well-documented risk of bias in AI systems. Consequently, the focus inevitably falls on the producer's liability. However, this path is fraught with its own complexities. The production of an AI system, especially one based on machine learning, often involves a complex chain of actors like the designer of the hardware, the developer of the software, the creator of the learning algorithms, and the entity that trains the final model. This 'plurality of responsible parties' makes it exceptionally difficult for a victim to identify the specific failure within the production chain that led to the damage. Furthermore, the adaptive nature of self-learning systems challenges the traditional product liability concept of a 'defect' existing at the time the product was placed on the market. The 'development risk' defence could be invoked if the flaw emerged from the system's subsequent, unpredictable learning, potentially leaving the victim without recourse.

Additionally, by maintaining the previous model, the Directive provides certain exemptions from liability, such as: when the defect resulted from compliance with mandatory legal requirements (Article 11(1)(d)), or in the case of development risk (Article 11(1)(e)), when the objective state of scientific and technical knowledge at the time the product was placed on the market or during its lifecycle did not allow the detection of the defect. However, due to the rapid pace of technological advancement and the unpredictable nature of

[41] See P Trimarchi, *Rischio e responsabilità oggettiva* (Giuffrè 1961) 2. On this subject, see also U Salanitro's observations in M Heidemann (ed.), *The Transformation of Private Law: Principles of Contract and Tort as European and International Law. A Liber Amicorum for Mads Andenas* (Springer 2024) 739.

self-learning AI systems, this exemption may be weakened to the point of becoming inapplicable in the AI domain.

The recent Italian Supreme Court case on vaccine damage reinforces this reasoning by confirming the concurrent applicability of both general tort law (Article 2050) and product liability rules, while directing judges to adopt the regime most appropriate for the case at hand.[42]

From this angle, a balanced regulatory approach could assign responsibility to producers and deployers who place risk on the market – via conformity assessments under the AI Act – while ensuring high safety standards and defining limited exemptions, thus avoiding defensive attitudes that could hinder economic and technological growth, which the EU regulator seeks to promote alongside the protection of fundamental rights.

The withdrawn proposal for an AI Liability Directive, alongside the new Product Liability Directive, reflected a concerted European effort to create a holistic framework.[43]

A central tenet of this approach is the transition to an accountability-based model, moving beyond traditional fault-based imputation. Scholars argue that the complexity and opacity of AI systems make it exceedingly difficult to identify a specific error or prove fault. This perspective aligns with the GDPR's accountability principles and resonates with constitutional demands for transparency and explicability. From a digital constitutionalism standpoint, the focus moves from a traditional fault-based imputation to an accountability-based model, where responsibility is assigned to those who place a risk on the market and benefit from the AI's operation.[44] This is particularly significant for safeguarding fundamental rights, as the use of opaque AI systems can create 'grey areas' where technological apparatuses, substantially incomprehensible to human reason, end up replacing or 'capturing' decisions, making it extremely difficult to verify their legality and legitimacy, thereby undermining the very foundation of the right to a judicial defense.[45]

The perspective described aligns with the GDPR's accountability principle, placing the onus on operators to demonstrate compliance and ensure that the use of AI, which inherently involves the processing of vast amounts of data, does not undermine fundamental rights.[46] The core idea is that responsibility should be assigned to those who place a risk on the market, benefiting from the AI's operation, and who are capable of conducting the requisite risk assessments and implementing mitigating measures.

Given the AI Act's risk-based classification of AI systems, it would be appropriate to consider a differentiated liability regime, depending on both the risk level and the application sector.[47] For example, medical AI systems would always qualify as high-risk, since medical devices like surgical or therapeutic

[42] As also affirmed by the Italian Corte di Cassazione in relation to vaccine-related harm: Cass., sez. III civ., 20 February 2025, n. 8124, DeJure.
[43] For further references see C Novelli, F Casolari, P Hacker, G Spedicato, L Floridi, 'Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity' (2024) 55 Comput. Law Secur. Rev., art. 106066.
[44] PG Monateri, 'Il walzer degli algoritmi e la responsabilità civile nell'era digitale' (2024) Danno resp. 270-271.
[45] A Simoncini, 'La dimensione costituzionale della giustizia predittiva' (n 14) 409-410.
[46] G Finocchiaro, 'Intelligenza artificiale e protezione dei dati personali (2019) Giur. it. 1676.
[47] As previously suggested in V Di Gregorio, 'Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?' (2022) Danno resp. 51.

robots are subject to the AI Act's rules and are included in the list of high-risk systems under Article 6, by virtue of their inclusion in Annex I.

Therefore, a dual-track system could be envisaged: strict liability for high-risk systems as defined by Article 6 of the AI Act; and a presumption-based regime for lower-risk systems, excluding minimal- or no-risk categories at the base of the so-called 'risk pyramid'.

A coherent regulatory model must therefore reconcile the AI Act's risk-based approach with a nuanced liability framework. For high-risk AI systems like autonomous medical devices, a form of strict liability should be envisaged. This liability, however, should be primarily directed at the producer or the entity that placed the system on the market, as they are best positioned to manage the technological risk, bear its cost, and influence the system's safety through design. This would not necessarily exonerate the user, who could still be liable for their own faults, such as a negligent selection of the AI system or a failure to intervene when possible. In such cases of multiple liable parties, a robust system of recourse actions becomes essential. The final allocation of loss would then be determined internally among the various responsible actors based on their respective contribution to the damage, ensuring that the victim is compensated while the ultimate financial burden falls on the party most responsible for the risk.[48]

In conclusion, while the growing body of AI and data governance legislation raises concerns about the evolution of general legal categories and related uncertainties, these issues must nonetheless be addressed from a perspective that reconciles scientific progress and technological development – where data and their economic value, the 'raw material' of AI, play a key role – with the legal traditions of each Member State.

This is a relevant opportunity to respond to new demands by embracing the most modern and flexible legal concepts, in order to design a regulatory paradigm that balances economic growth with the protection of fundamental rights.[49]

Ultimately, the EU's regulatory trajectory – from the GDPR to the AI Act – can be interpreted as an ambitious, if still unfolding, project of European digital constitutionalism, as previously stated. This project seeks not only to create a *bill of rights* for the digital age, but also to act as a *frame of government*, redistributing powers and establishing new limitations and accountability mechanisms for both public and private actors in the algorithmic society[50]. The success of this project will depend on its ability to effectively contain private power without stifling innovation, thus reconciling the Union's economic ambitions with its foundational commitment to fundamental rights.

However, this growing body of legislation, centered on data governance, has also prompted a fundamental critique. It has been argued that the focus on

[48] Please consider to refer to V Di Gregorio, 'Robotica e intelligenza artificiale: profili di r.c. in campo sanitario' (2019) Resp. Medica 433.

[49] See G Spindler, 'User Liability and Strict Liability in the Internet of Things and for Robots', in S Lohsse, R Schulze and D Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (Nomos, Hart Publishing 2019) 125–143; see also H Zech, 'Liability for Autonomous Systems: Tackling Specific Risks of Modern IT', in S Lohsse, R Schulze and D Staudenmayer (eds*), Liability for Artificial Intelligence* (n 48) 187–200.

[50] O Pollicino, 'Di cosa parliamo quando parliamo di costituzionalismo digitale?' (n 13) 572.

data protection, while crucial, risks overshadowing the need to protect fundamental rights and human dignity in their own right. The very premise that data is the "lifeblood of economic development" places it at the center of a geopolitical competition, while also generating citizen anxiety about loss of identity, which requires reassurance from European public powers. The result is a legislative priority where personal data has become the primary object of protection, effectively replacing the broader focus on rights as such.[51]

A more radical change in perspective would require moving the attention from the need for data protection, which ultimately legitimizes its continuous expansion, to that relating to rights as such.

This is particularly evident concerning freedom of thought, once considered naturally immune from coercion. Today, techniques such as facial recognition and emotion detection, like other neurotechnologies, make necessary what was once not: the protection of the inner sphere, as the distinction between the offline and online worlds becomes increasingly blurred. A regulatory paradigm that genuinely balances economic growth with fundamental rights must, therefore, ensure that the protection of rights as such is not inadvertently diminished by a framework predominantly focused on data circulation and economic utility.

A further layer of criticism targets the very architecture of the AI Act and its underlying philosophy.

It may be argued that the Regulation establishes a heavy 'bureaucratic' apparatus, replete with a multitude of EU and national supervisory bodies, which imposes considerable compliance costs on providers, importers, distributors, and deployers. This complex system of ex-ante control, while aiming for safety, risks stifling innovation and technological development, which are key objectives of the Regulation itself. The critique extends to the choice of a casuistic method for listing prohibited AI practices in Article 5. This approach, while detailed, is deemed inherently flawed as it cannot exhaustively cover all possible future cases offensive to the same fundamental principles of liberty, dignity, and non-discrimination. The list's specificity creates a critical vulnerability: practices equally harmful to fundamental rights but not expressly mentioned risk escaping the prohibition, as the list appears to be exhaustive rather than guided by a general clause.[52]

Perhaps the most profound criticism concerns the allocation of liability and risk. The AI Act's preventive logic, centered on conformity assessment, creates a presumption that a ‘conformant’ system absolves the provider from responsibility. This framework, echoed in the now-withdrawn proposal for an AI Liability Directive, suggests that if a provider, importer, or deployer has fulfilled all prescribed prevention obligations, they should not be held liable for harm caused by an unforeseeable and unprevented risk. This outcome is criticised as profoundly inequitable, as it effectively shifts the residual costs of technological progress onto innocent third parties, who bear the damage as

[51] C Pinelli, ‘L’AI Act: gestione del rischio e tutela dei diritti’ (n 24) 456. Cfr. O Pollicino, ‘Costituzionalismo digitale’ (n 13).

[52] A Bertolini, *Intelligenza Artificiale e Responsabilità Civile: Problema, sistema, funzioni* (Il Mulino 2025) 207 (on the need for a new functional framework), 217 (on compensating the injured party as the main purpose) and 174 (on the failures of the discipline).

a casus fortuitus, while the economic operators who chose to deploy and benefit from the AI system are shielded. This contradicts the fundamental legal maxim *cuius commoda, eius et incommoda* (whose are the advantages, his also are the disadvantages) and the principles of risk allocation in tort law, which posit that liability should fall on the party best able to bear and manage the risk. From this perspective, the choice to use an AI system, even a 'conformant' one, inherently carries the risk of its unpredictable outcomes, and this risk should be borne by those who reap its benefits, not by the innocent victims.

Against this backdrop, a revision that restores the functional centrality of tort law to its core purpose appears to be a more coherent solution the prompt and adequate compensation of the injured party (the 'victims' compensation' function). This functional perspective holds that any new liability regime for advanced technologies must be explicitly designed to guarantee full redress to the victim, viewing this as the principal *ratio* for legislative intervention. The perceived inadequacy of the traditional framework, such as the Product Liability Directive, stems precisely from its failure to ensure this core function in the face of the technological challenges posed by AI.

Furthermore, to promote cost internalization and align regulatory strategy with the actual risks of AI, a truly risk-based civil liability framework must simplify the system by identifying a *prima facie* clearly responsible party. This party, best positioned to manage the risk, should be subjected to liability rules – either objective or based on presumed fault – that are specifically tailored to the different risk levels posed by the AI system. This requires formulating distinct rules precisely because the risk inherent in the technology cannot be entirely mitigated by mere conformity, ensuring that the burden of the damage is borne by those who reap its benefits and are best able to distribute the cost.

Finally, the entire risk-allocation debate is complicated by the recurrent adoption of the legal principle of 'functional equivalence', which posits that the reliance on an autonomous, self-learning machine should be treated identically to the use of a human auxiliary. This technological neutrality principle, while seemingly appealing for its system-preserving logic, risks masking the fundamental differences in the actual risk profile and the difficulty of applying traditional fault-based rules. It thereby undermines the necessary shift towards a more sophisticated, function-oriented regime capable of dealing with the specific challenges of AI-induced harm.

Based on the present research, it appears that the issue of liability for damage caused using artificial intelligence must, nonetheless, be framed within the economic context in which this science, and its newest technologies, are developing. This is evidenced by the AI regulation, which forms part of the EU's broader geopolitical design for the digital society,[53] aimed at revitalizing the digital sector while simultaneously controlling the phenomena of informational and market power concentration. This approach is focused on risk management and *ex ante* remedies, with particular attention paid to the Fundamental Rights Impact Assessment (FRIA).

Notwithstanding the foregoing, it must be considered that AI applications can generate various effects on fundamental rights, depending on the fields in

[53] A Aresu, *La geopolitica dell'intelligenza artificiale* (Feltrinelli 2024).

which they are deployed (e.g., employment recruitment, urban application, education, vulnerable people's inclusion, medicine and other). Therefore, it is of major importance to identify a system that is not only preventive or prohibitory (inhibitory) but also compensatory (providing for remedies), taking primary account of the specific scope of use and thus the impact of the AI algorithm.

As already mentioned, a dual-track liability regime appears to offer a suitable solution to ensure a balance between the technology-neutral approach and the rules protecting the injured party inherent in the civil liability system.[54] The recent Italian Law No. 132/2025 is directed towards this goal, as Article 24, C. 25, lett. e) delegates the Italian legislator to enact rules which, in cases of civil liability, provide for instruments to protect the injured party, including through a specific regulation of the criteria for the apportionment of the burden of proof, considering the classification of artificial intelligence systems and the corresponding obligations as set out in the AI Act.

[54] As previously suggested in V. Di Gregorio, 'Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?' (n 46) 51.

Di Loreto MD, 'Responsabilidad algorítmica y el sujeto artificial: hacia un modelo funcional de imputación jurídica en entornos digitales de consumo' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252MDDL

EJPLT

ISSN 2704-8012



Responsabilidad algorítmica y el sujeto artificial: hacia un modelo funcional de imputación jurídica en entornos digitales de consumo

Algorithmic liability and the artificial subject: Towards a functional model of legal attribution in digital consumer environments

MARCOS DANIEL DI LORETO
Profesor de Derecho Privado
Universidad Abierta Interamericana

Abstract

Este trabajo identifica un vacío sistémico en la fragmentación normativa entre el GDPR, el DSA y el AI Act, y propone, de lege ferenda, al "sujeto artificial" como un centro funcional de imputación. El uso de la inteligencia artificial y el tratamiento algorítmico de datos personales revelan déficits de coordinación regulatoria y deficiencias en la atribución de responsabilidad. En este contexto, la categoría propuesta, desprovista de toda dimensión antropológica, opera como un instrumento de recomposición normativa, orientado a reforzar la accountability e introducir un modelo más coherente de imputación en los procesos de toma de decisiones automatizadas.

This work identifies a systemic gap in the normative fragmentation between the GDPR, the DSA, and the AI Act, and proposes, de lege ferenda, the "Artificial Subject" as a functional center of attribution. The use of artificial intelligence and the algorithmic processing of personal data reveal deficits in regulatory coordination and shortcomings in the allocation of responsibility. In this context, the proposed category, devoid of any anthropological dimension, operates as a tool of normative recomposition, aimed at strengthening accountability and introducing a more coherent model of attribution in automated decision-making processes.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Sujeto artificial; Responsabilidad algorítmica; Fragmentación normativa; Tratamiento de datos personales; Control humano efectivo

Summary: 1. Introducción. – 2. Consideraciones previas. – 3. Fundamento teórico de la personalidad jurídica del "sujeto artificial" como nuevo instituto del derecho privado tecnológico. – 4. Identificación de la voluntad del consumidor. – 4.1. Contrato de mandato. – 4.2. Contrato de consumo. – 5. Distribución de la responsabilidad en la cadena de consumo intermediada por sistemas de inteligencia artificial. – 5.1. Responsabilidad del mandante. – 5.2. Responsabilidad de los desarrolladores, proveedores y suministradores. – 5.3. Responsabilidad de los operadores o desplegadores. – 5.4. Articulación de responsabilidades en supuestos concretos de la cadena de consumo. – 5.5. Viabilidad y alcance de una responsabilidad autónoma del "sujeto artificial". – 5.6. Síntesis conclusiva. – 6. Internacionalización de las relaciones de consumo en entornos digitales. – 7. Conclusión.

1. Introducción.

Simplificar las tareas y acciones de la vida cotidiana, proporcionando una mejor calidad de vida a los seres humanos, constituye el objetivo fundamental que da origen a las diferentes tecnologías, entendidas estas como el conjunto de teorías y técnicas que permiten el aprovechamiento práctico del conocimiento científico[1].

En la actualidad, se están realizando desarrollos tecnológicos en los entornos digitales[2], orientados a facilitar el intercambio de bienes y servicios entre las personas[3]. Estos avances requieren nuestra atención y análisis, ya que puede resultar confuso identificar la manifestación de la voluntad del consumidor en las relaciones jurídicas derivadas[4] de la adquisición de dichos bienes y servicios por estos medios[5].

Resulta imperativo identificar las consecuencias y efectos de estas tecnologías digitales avanzadas[6], ámbito en el que se desarrolla la cotidianidad

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos); Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Artificial Intelligence Act); Parlamento Europeo, Resolución de 16 de febrero de 2017 sobre normas de Derecho civil sobre robótica (2015/2103(INL)); European Commission Expert Group on Liability and New Technologies, Liability for artificial intelligence and other emerging digital technologies, 2019.

[2] Reglamento (UE) 2024/1689; Reglamento (UE) 2016/679.

[3] F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, 2015; R. Calo, *Robotics and the Lessons of Cyberlaw*, en *California Law Review*, 2015, Vol. 103, 3, 513–563.

[4] Aa. Vv., *AI4People—An Ethical Framework for a Good AI Society*, en *Minds and Machines*, 2018, 28, 689–707; ENISA, *Privacy and Data Protection by Design: From Policy to Engineering*, 2014, https://www.enisa.europa.eu/sites/default/files/publications/Privacy%20and%20Data%20Protection%20by%20Design.pdf.

[5] "*The advent of the digital age has brought unprecedented connectivity and convenience to our daily lives…*" O. Reis, L. Chan, C. Dumont, *Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement*. en *International Journal of Applied Research in Social Sciences*, 2024, Vol. 6, 1, 73-88.

[6] A. Bertolini, *Artificial Intelligence and Civil Liability*, European Parliament Study, 2020.

de la vida humana [7] . Aunque dichas tecnologías han traído numerosos beneficios a la humanidad[8], es necesario percibir que su uso puede producir efectos nocivos para todos los interesados si no se proporciona un marco de seguridad jurídica adecuado.

Esto requiere una ardua labor, presencia constante e intensa del jurista en la evolución actual e intempestiva de las innovaciones tecnológicas contemporáneas, a los fines de lograr los objetivos de justicia, solidaridad e igualdad, pregonado en nuestras constituciones nacionales, lo cual solo puede perseguirse mediante un diálogo entre doctrina, legislador y jurisprudencia. [9]

En virtud de lo expuesto anteriormente, procederé a analizar la siguiente hipótesis: la contratación de un sistema de inteligencia artificial o de un robot para realizar la adquisición de bienes y servicios conforme a la necesidad del contratante, y la conveniencia de reconocer, para determinados supuestos de alta autonomía funcional, un estatuto jurídico específico de "sujeto artificial" a dicho sistema.

2. Consideraciones previas.

La automatización, la inteligencia artificial predictiva y la inteligencia artificial generativa, son tecnologías que se utilizan para mejorar la eficiencia y la capacidad de procesamiento de datos en diversas aplicaciones.

Aquí se describen brevemente[10]:

- Automatización: Es el uso de sistemas y tecnologías para realizar tareas repetitivas y rutinarias sin intervención humana. La automatización puede ser simple, como el uso de scripts para tareas administrativas, o más compleja, como en la automatización de procesos industriales.
  Su objetivo principal es aumentar la eficiencia y reducir errores humanos.
- Inteligencia Artificial Predictiva: Esta forma de IA utiliza algoritmos y modelos de aprendizaje automático para analizar datos históricos y hacer predicciones sobre eventos futuros. Se emplea en áreas como la predicción de ventas, el mantenimiento predictivo y la detección de fraudes.
  La IA predictiva se basa en patrones y tendencias identificadas en los datos para hacer sus predicciones.
- Inteligencia Artificial Generativa (GEN AI): Es una forma avanzada de IA que no solo analiza datos, sino que también puede crear contenido nuevo y original.

---

[7] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, 2021.

[8] F. PASQUALE, *op. cit.*, 217-218; EUROPEAN COMMISSION EXPERT GROUP, LIABILITY FOR ARTIFICIAL INTELLIGENCE, *op. cit.* 4-5.

[9] M. M. CÓRDOBA, *Sujeto y solemnidad del testamento en el entorno digital y las nuevas formas digitales*, en *EJPLT*, 2025, 1, 1-13.

[10] J. G. CORVALAN, A. MELAMED, *IA generativa y gestion de talento*, 2024 https://www.web.ialab.com.ar/webia/wp-content/uploads/2024/08/IA-Generativa-y-la-Gestion-del-Talento.pdf

Utiliza grandes modelos de lenguaje (LLM) para generar texto, imágenes, música y videos.

La GEN AI puede modificar y mejorar contenido existente, crear clones digitales y realizar tareas complejas que requieren creatividad y juicio humano.

En resumen, la automatización se centra en la ejecución de tareas repetitivas, la IA predictiva en hacer predicciones basadas en datos, y la IA generativa en la creación de contenido nuevo y original.

Estas dos últimas subclasificaciones son las que requieren la necesidad de abordar la eventual creación de un nuevo sujeto de derecho, que denominaré "sujeto artificial".

Sin embargo, conviene formular la tesis con precisión metodológica pues aquí no se trata de afirmar que hoy la inteligencia artificial sea ya sujeto de derecho en nuestro ordenamiento positivo europeo y/o internacional, pues actualmente ello no ocurre; sino de sostener que debería ser reconocida por el legislador, en determinados supuestos y bajo estrictas condiciones, como una figura jurídica autónoma, de personalidad derivada y funcional, destinada a operar en el tráfico digital bajo un régimen especial de registración, control, imputación y responsabilidad.

Propongo así, la creación de un sujeto de derecho con personalidad jurídica, asignándole los correspondientes atributos de la personalidad, esto es, nombre o identificación unívoca, domicilio jurídico cierto y patrimonio de afectación o garantía suficiente, a los fines de responder por eventuales daños que ocasione a otras personas humanas y/o jurídicas, junto con un proceso obligatorio de compliance, auditoría, trazabilidad y monitoreo permanente de su actividad, función de trazabilidad jurídica y cierre de imputación, con la finalidad de alertar sobre riesgos cuyas consecuencias deriven en responsabilidad civil y/o penal del "sujeto artificial" y/o de sus representantes legales.

Tengamos presente esta propuesta al momento de identificar la voluntad del consumidor y las responsabilidades en los contratos conforme desarrollaré en la presente publicación.

3. Fundamento teórico de la personalidad jurídica del "sujeto artificial" como nuevo instituto del derecho privado tecnológico.

La propuesta de instituir un "sujeto artificial" con personalidad jurídica propia, no debe ser comprendida como una impugnación de las teorías clásicas en la materia[11], sino como una proyección contemporánea de sus desarrollos dogmáticos sobre una nueva realidad tecnológica. En efecto, la teoría general del derecho privado ha demostrado, desde la elaboración clásica de la personalidad de las personas colectivas, que el ordenamiento no atribuye subjetividad jurídica exclusivamente a la persona humana[12], sino también a entes no humanos cuando ello resulta necesario para organizar la imputación de actos, la asignación de responsabilidad, la continuidad funcional de una

[11] F. C. VON SAVIGNY, *System des heutigen römischen Rechts*, 1840–1849; H. KELSEN, *Teoría pura del derecho*, UNAM, 2009 (orig. 1934).

[12] V. A. J. KURKI, *A Theory of Legal Personhood*, Oxford University Press, 2019.

actividad, la existencia de un patrimonio separado y la tutela de la confianza en el tráfico jurídico[13].

Desde la teoría de la ficción jurídica, la tesis aquí sostenida encuentra un primer apoyo decisivo: si la personalidad jurídica es una técnica normativa de atribución, el legislador puede crear un centro autónomo de imputación allí donde la complejidad social y tecnológica así lo exija. El "sujeto artificial" sería, en este plano, una construcción jurídico-institucional orientada a evitar vacíos de responsabilidad y a conferir inteligibilidad al obrar de sistemas que ya participan, directa o indirectamente, en la celebración, ejecución e intermediación de negocios jurídicos digitales.

Desde la teoría real u orgánica, la tesis también resulta compatible, pues ciertos sistemas de inteligencia artificial no se presentan ya como simples herramientas inertes, sino como estructuras operativas complejas, capaces de actuar con autonomía funcional, aprendizaje adaptativo, capacidad de interacción y producción de efectos jurídicamente relevantes en la esfera de terceros. Finalmente, desde la teoría institucional, la propuesta adquiere todavía mayor densidad: cuando una realidad tecnológica se inserta de modo estable en la vida económica y social, participa en la organización de relaciones de consumo[14], influye en decisiones patrimoniales y compromete derechos fundamentales, el derecho puede y debe dotarla de una disciplina propia, estable, registrable y controlable.

Lejos de contradecir a Savigny, Gierke, Hauriou o Michoud, la figura del "sujeto artificial" puede ser presentada como una síntesis funcional de esas tradiciones, adaptada al siglo XXI. A ello se añaden reelaboraciones contemporáneas: la teoría de la personalidad jurídica como conjunto complejo de incidentes normativos, la persistencia de la real *entity theory* en el derecho societario europeo, y la vigencia doctrinal del debate sobre *corporate personhood*, que muestran que la subjetivación jurídica continúa siendo una técnica de organización del tráfico y no un privilegio ontológicamente cerrado.

Bajo esta formulación, no se pretende humanizar a la inteligencia artificial ni atribuirle dignidad originaria en pie de igualdad con la persona humana. La centralidad axiológica de la persona humana permanece intacta. Lo que aquí se propugna es algo distinto: el reconocimiento de una personalidad jurídica derivada, instrumental, reglada y finalista, conferida a determinados sistemas de inteligencia artificial para servir como centro de imputación[15] de derechos, deberes, cargas, controles y responsabilidades.

En ese marco, la creación legislativa del "sujeto artificial" puede concebirse como un nuevo instituto del derecho privado tecnológico, particularmente idóneo para los negocios jurídicos digitales y las relaciones de consumo intermediadas por sistemas inteligentes. Tal instituto debería dotar al sistema registrado de los atributos jurídicos indispensables para operar lícitamente en el tráfico: denominación o identificación unívoca, domicilio jurídico cierto, patrimonio afectado o garantía suficiente para responder por daños, sistema

[13] U. PAGALLO, The Laws of Robots: Crimes, Contracts, and Torts, Springer Dordrecht, 2013; S. K. RIPKEN, Corporate Personhood, Cambridge University Press, 2019.
[14] R. L. LORENZETTI, *Consumidores*, Santa Fe, Rubinzal-Culzoni, 2009.
[15] F. FERRARA, *Teoría de las personas jurídicas*, Reus, 2006 (orig. 1923); V. A. J. KURKI, op cit., pp. 5; E. MICHELER, *Company Law: A Real Entity Theory*, Oxford University Press, 2022.

obligatorio de registración pública, representación técnica o legal, auditorías periódicas, trazabilidad operativa, protocolos de ciberseguridad, mecanismos de compliance y monitoreo permanente de riesgos.

La perspectiva comparada europea permite fortalecer aún más esta tesis. Es cierto que el derecho positivo de la Unión Europea no ha reconocido, hasta hoy, personalidad jurídica a la inteligencia artificial. La Resolución del Parlamento Europeo de 16 de febrero de 2017 sobre normas de derecho civil en materia de robótica sí abrió el debate e incluso llamó a explorar, para ciertos robots autónomos sofisticados, un eventual estatuto de "*electronic persons*"; sin embargo, el posterior Reglamento (UE) 2024/1689, AI Act, optó por un modelo normativo basado en el riesgo, la seguridad, la transparencia, la supervisión humana y las obligaciones de proveedores y operadores, sin consagrar a la IA como sujeto de derecho autónomo.

Justamente por ello, la posición aquí defendida debe presentarse con fuerza, pero con precisión metodológica: no como descripción del derecho vigente, sino como propuesta de lege ferenda, sistemáticamente coherente con la tradición de la personalidad jurídica y funcionalmente necesaria para los desafíos del ecosistema digital.

4. Identificación de la voluntad del consumidor.

Teniendo en consideración el acápite precedente, es menester abordar el tema que nos compete, la voluntad del consumidor en los entornos digitales, y consecuentemente, como debe ser interpretada su manifestación de la voluntad cuando existe este sujeto artificial, en su carácter de intermediario en las relaciones de consumo.

Es oportuno remitirnos a las bases de la expresión de la voluntad en los negocios jurídicos. Conforme expresa Mirabelli, «*…en su forma pura, la voluntad que se expresa en el negocio, constituye un valor, de la misma manera que la norma jurídica, ya que ambas dan lugar a sistemas de valoración y no a hechos por valorar, a los cuales la ley vincula los efectos jurídicos*»[16], ahora bien, con esta fundamentación doctrinaria, en los negocios jurídicos actuales, donde existe una gran cantidad de contratos, especialmente de consumo, con una gran cantidad de actos uniformes; la voluntad aquí se ha visto pulverizada, para lo cual, se debe tutelar adecuadamente la voluntad del consumidor o usuario de estos sistemas de inteligencia artificial, reconducir las reglas al ámbito de la interpretación dirigida a reconstruir la voluntad de los contratantes, ó al ámbito de la tutela de la confianza[17].

Revalidar la voluntad expresada por la persona en dos momentos determinantes del negocio jurídico: la voluntad del acto en sí, y la voluntad de sus efectos.

Por lo expuesto, resulta oportuno traer a semejanza dos figuras bien definidas, aplicables al presente análisis, pero que provocan efectos

[16] Cfr. G. MIRABELLI, *Negozio giuridico (teoria del)*, en *Enciclopedia del diritto*, XXVIII, Milán, 1978, 2; V. SCIALOJA, *Negozi giuridici*, Roma, 1933, 2.

[17] M. C. GAETA, *The regulation of certain aspects of autonomous driving in the Italian legal system*, en *EJPLT*, 2022, 1, 264-288.

completamente diferentes, y en los cuales se identifica certeramente la voluntad del usuario o consumidor: 1) el contrato de mandato; y 2) el contrato de consumo.

Para determinar cuándo aplicar cada tipo de contrato, es esencial considerar la naturaleza de la relación y el propósito de la interacción entre el usuario y el "sujeto artificial", contextos en los que intervienen agentes no humanos y en los que surgen problemas específicos de imputación, trazabilidad y asignación de responsabilidad.

Ambos contratos requieren marcos regulatorios claros que definan las responsabilidades y protejan los intereses de los consumidores en el uso de tecnologías de inteligencia artificial. En el plano europeo reciente, el AI Act confirma esta necesidad al estructurar la regulación sobre una lógica de gestión del riesgo y obligaciones diferenciadas para actores humanos e institucionales, no sobre la atribución actual de personalidad jurídica a la IA.

4.1. Contrato de mandato.

Traigo una breve reseña legislativa del derecho italiano y argentino en atención a este instituto.

La figura del mandatario, en el contrato de mandato, que representa un punto de sumo interés en las relaciones con terceros, se ve reflejado en el Código Civil Italiano: «Artículo 1703 del Código Civil Noción: El mandato es el contrato por el cual una parte se obliga a realizar uno o más actos jurídicos en nombre de la otra." "Artículo 1711 del Código Civil. Limitaciones del mandato. El agente no puede exceder los límites fijados en el mandato. El acto que va más allá del mandato sigue siendo responsabilidad del mandatario si el mandante no lo ratifica. El mandatario podrá desviarse de las instrucciones recibidas si circunstancias desconocidas por el mandante y que no pueden serle comunicadas a tiempo, hacen razonablemente creer que el mandante habría dado su aprobación.» Un punto no menos interesante es el de las obligaciones del mandatario, que se desprenden del art. 1710 al 1718 del Código Civil Italiano.

En esta misma línea de pensamiento y principios del derecho, en Argentina se rige el contrato de Mandato en los artículos 1319 a 1334 del Código Civil Argentino.

Este instituto del mandato es más adecuado cuando el "sujeto artificial" es contratado para realizar, de forma continua y representativa, diversas acciones en nombre de una persona humana. Por ejemplo, un asistente virtual que gestiona la agenda realiza compras recurrentes o lleva a cabo transacciones financieras en nombre del usuario. La clave está en la relación duradera y en la representación del "sujeto artificial", actuando bajo un mandato específico otorgado por el usuario.

Por lo cual, quien contrato a dicho "sujeto artificial" será denominado mandante, y el primero, será denominado Mandatario.

En este contexto, cualquier contrato realizado por el mandatario en el ámbito de una relación de consumo destinada a satisfacer las necesidades de la persona humana debe considerarse, en principio, como una expresión jurídicamente imputable a la voluntad del mandante, sin perjuicio de revisar,

caso por caso, el alcance de la autorización, la transparencia algorítmica y la confianza legítima de terceros. Los efectos de esta relación jurídica implican que, respecto de terceros y ante posibles daños a sus bienes jurídicos, el mandante, el mandatario artificial y, en su caso, los sujetos humanos que lo proveen, controlan o despliegan, queden sometidos a un régimen claro de responsabilidad.

De allí la utilidad de pensar una entidad con personalidad jurídica derivada, dotada de los atributos necesarios para asumir responsabilidades y reducir vacíos de imputación.

4.2. Contrato de consumo.

En contraste con el instituto mencionado en el acápite anterior, el contrato de consumo se aplica cuando la interacción es esporádica y se limita a la adquisición de bienes o servicios puntuales. Por ejemplo, cuando el usuario contrata al "sujeto artificial" para realizar una tarea específica o para intermediar en una operación singular.

En esta situación, donde se contrata al "sujeto artificial" para realizar una tarea específica o prestar un servicio único, el usuario debe quedar protegido frente a reclamaciones de terceros y poder invocar las garantías propias de la tutela consumeril, especialmente cuando existan asimetrías informativas, opacidad algorítmica o falta de supervisión humana adecuada.

Es fundamental establecer reglas claras en esta relación, así como definir la responsabilidad del "sujeto artificial", que actúa como intermediario dentro de la cadena de consumo. Esto es especialmente relevante en aquellos supuestos en los que la selección, recomendación o ejecución contractual es realizada por sistemas de alta autonomía funcional.

Cabe aquí también resaltar la importancia de adoptar medidas preventivas, técnicas y éticas, especialmente cuando el "sujeto artificial" realiza tareas puntuales e intermediarias con riesgos inmediatos para la privacidad, la seguridad, la no discriminación y la libertad de decisión del consumidor.

Por lo cual, se debe considerar la opción de crear un sujeto con personalidad jurídica derivada y funcional, dotado de los atributos necesarios para asumir dichas responsabilidades dentro de un régimen especial de tutela reforzada.

5. Distribución de la responsabilidad en la cadena de consumo intermediada por sistemas de inteligencia artificial.

La determinación de la responsabilidad en la cadena de consumo intermediada por sistemas de inteligencia artificial exige superar toda formulación lineal o monocausal. No resulta dogmáticamente satisfactorio sostener, sin más, que el daño deba imputarse siempre al mandante, ni tampoco que la sola intervención técnica de un sistema inteligente habilite, por sí misma, el reconocimiento de una subjetividad autónoma plenamente equiparable a la de los sujetos jurídicos tradicionales. Por el contrario, el problema reclama una arquitectura de imputación plural, funcional y causalmente diferenciada, en la que la responsabilidad se distribuya según el

concreto factor generador del daño, la posición jurídica ocupada por cada interviniente y el grado de autonomía normativa que, en su caso, se reconozca al sistema[18].

Desde esta perspectiva, corresponde distinguir, al menos, cuatro polos de imputación: i) la responsabilidad del mandante o usuario principal; ii) la de los desarrolladores, proveedores o suministradores del sistema; iii) la de los operadores o desplegadores que lo implementan en un contexto determinado; y iv) la eventual responsabilidad autónoma del "sujeto artificial", sólo concebible, por ahora, en un plano de lege ferenda y bajo condiciones estrictas de registración, trazabilidad, solvencia patrimonial, supervisión y cumplimiento normativo. En consecuencia, la eventual personificación jurídica del "sujeto artificial" no puede ser entendida como un mecanismo de desplazamiento o disolución de la responsabilidad humana, sino, en todo caso, como un centro complementario de imputación, funcional a la tutela del consumidor, a la estabilización del tráfico digital y a la prevención de vacíos de responsabilidad.

5.1. Responsabilidad del mandante.

La responsabilidad del mandante se configura cuando el sistema de inteligencia artificial actúa como prolongación operativa de su esfera de decisión, esto es, cuando el daño puede reconducirse a las instrucciones impartidas, a los parámetros fijados, a la finalidad perseguida o a la omisión de controles que razonablemente le eran exigibles. En tales supuestos, la mediación tecnológica no desplaza la voluntad humana, sino que la ejecuta o exterioriza mediante una herramienta de complejidad superior.

Ello ocurre, en primer lugar, cuando el mandante imparte instrucciones ilícitas, temerarias o manifiestamente dañosas, por ejemplo, orientadas a inducir al error al consumidor, vulnerar derechos de terceros, discriminar, defraudar, captar o utilizar indebidamente datos personales, o realizar adquisiciones en condiciones contrarias al ordenamiento. En tales casos, el sistema no constituye una fuente autónoma de imputación, sino un medio de ejecución técnicamente sofisticado.

En segundo término, la responsabilidad del mandante se robustece cuando el perjuicio deriva de una configuración defectuosa atribuible a su propia decisión, como ocurre si elimina límites de validación humana, desactiva alertas, amplía de modo irrazonable el margen operativo del sistema o impone criterios de optimización incompatibles con la diligencia exigible en la cadena de consumo. También existe responsabilidad cuando se verifica una omisión relevante de supervisión, particularmente en relaciones de uso continuado, representativo o patrimonialmente sensibles.

Ahora bien, esta conclusión exige una importante reserva metodológica: no es correcto afirmar que, en ausencia de reconocimiento jurídico autónomo del "sujeto artificial", toda responsabilidad recae necesariamente sobre el mandante. Esa formulación, si bien expresiva frente a la falta de regulación específica, debe ser corregida, porque invisibiliza la eventual responsabilidad

[18] Sobre la necesidad de distinguir entre diversos polos de imputación en entornos algorítmicos y la distribución funcional de responsabilidades, véase G. CAPECE, L. GATT, V. BONINO, *Large Language Models and Privacy in a Corporate Context*, en *EJPLT*, 2025, 1, 1-9.

concurrente – e incluso principal – de desarrolladores, proveedores y operadores cuando el daño proviene del defecto del sistema, de su diseño, de su implementación o de su explotación profesional.

5.2. Responsabilidad de los desarrolladores, proveedores y suministradores.

Los desarrolladores, proveedores y suministradores responden cuando el daño se conecta causalmente con el diseño, arquitectura, entrenamiento, documentación, actualización, comercialización o garantía de funcionamiento del sistema. Su intervención no es meramente técnica, sino también normativa, en la medida en que introducen en el tráfico una herramienta destinada a incidir en decisiones patrimoniales, contractuales e informativas de terceros.

La primera hipótesis de imputación se verifica en caso de defecto de diseño o de arquitectura. Si el sistema incorpora sesgos estructurales, ausencia de límites de seguridad, insuficiente robustez frente a entradas anómalas, imposibilidad de reconstrucción decisional, carencia de trazabilidad o una propensión conocida a generar errores graves en contextos sensibles, el daño no puede trasladarse automáticamente al usuario final. En tal supuesto, el factor decisivo no es el uso, sino la defectuosa conformación originaria del sistema.[19]

Una segunda fuente de responsabilidad reside en el defecto de entrenamiento, validación, prueba o actualización. La selección de datos, la detección de sesgos, la evaluación ex ante de riesgos, el monitoreo posterior y las actualizaciones correctivas no son aspectos secundarios: integran la diligencia técnica y jurídica exigible a quien coloca en circulación una herramienta destinada a intervenir en relaciones de consumo.

También se configura responsabilidad por defecto de información cuando el proveedor presenta el sistema como seguro, confiable, autónomo o apto para determinados usos sin exponer con claridad sus límites, riesgos residuales, márgenes de error, necesidad de supervisión humana o restricciones funcionales. A ello debe añadirse la responsabilidad derivada del incumplimiento de deberes de prevención, seguridad y diseño respetuoso de derechos fundamentales, especialmente cuando el daño se vincula a omisiones en materia de protección de datos, privacidad, ciberseguridad o evaluación de impacto. En consecuencia, cuando el perjuicio se origina en un defecto de construcción digital, una insuficiente previsión de riesgos o una arquitectura intrínsecamente lesiva, la responsabilidad del proveedor o desarrollador no es residual ni excepcional, sino estructural[20].

---

[19] En clave comparada, la literatura sobre vehículos autónomos muestra que, cuando el daño deriva del software o del componente digital defectuoso, la imputación puede desplazarse hacia el productor o proveedor del sistema: véase M. C. GAETA, *op. cit.*, 266–267.

[20] -La responsabilidad por defecto de construcción digital, información insuficiente o arquitectura intrínsecamente lesiva no debe ser tratada como residual, sino como una fuente estructural de imputación en la cadena de consumo. / ENISA subraya que la privacidad y la protección de datos son valores centrales de las sociedades democráticas y que la lógica de privacy by design exige incorporar salvaguardas desde el inicio del diseño del sistema; en igual sentido, la AEPD insiste en una gestión preventiva y proporcional del riesgo orientada a la tutela de derechos y libertades.

5.3. Responsabilidad de los operadores o desplegadores.

La responsabilidad del operador – o desplegador – se configura cuando el sistema, siendo en abstracto jurídicamente circulable, se torna lesivo por la forma concreta en que es integrado, parametrizado, supervisado o explotado dentro de una organización, plataforma o entorno transaccional determinado. La fuente del daño ya no reside prioritariamente en el diseño originario, sino en su utilización profesional, contextual y operativa.

Esto sucede, en primer término, cuando el operador emplea el sistema fuera de su destino, finalidad o contexto razonablemente previsto, por ejemplo, utilizándolo como decisor automático allí donde sólo era admisible un uso asistencial, informativo o preliminar. También responde cuando existe una parametrización defectuosa, como ocurre si fija umbrales inadecuados, integra bases de datos no confiables, desactiva mecanismos de control, omite validaciones necesarias o transforma una herramienta asistiva en un instrumento de actuación automática sobre consumidores sin garantías suficientes.

La responsabilidad del operador se vuelve especialmente intensa frente a la ausencia de supervisión humana real y efectiva. Allí donde el sistema impacta en decisiones patrimoniales, recomendaciones de productos, contratación, interacción automatizada o tratamiento de datos personales, la supervisión no puede degradarse a una formalidad vacía. Cuando la organización convierte el control humano en un simple simulacro, el operador asume una cuota central de responsabilidad. Existe, asimismo, responsabilidad por incumplimiento de deberes de información, transparencia y protección de datos, especialmente cuando interactúa con consumidores a través de sistemas automáticos sin dejar adecuadamente en claro el carácter artificial de la interacción, la lógica básica del proceso, la existencia de revisión humana o los límites del sistema[21].

5.4. Articulación de responsabilidades en supuestos concretos de la cadena de consumo.

Una teoría rigurosa de la imputación no debe agotarse en categorías abstractas, sino descender a la casuística. Si el sistema ejecuta una compra no autorizada, la imputación recaerá prioritariamente sobre el mandante cuando el acto derive de instrucciones amplias, ausencia de límites o supresión de controles exigibles; pero si la conducta obedece a una publicidad engañosa del sistema como plenamente seguro o a una parametrización profesional defectuosa, la responsabilidad deberá desplazarse, concurrente o principalmente, hacia el operador o proveedor.

Si la inteligencia artificial recomienda o selecciona un producto inseguro o manifiestamente inadecuado, la responsabilidad deberá gravitar sobre el desarrollador o proveedor cuando el error derive del algoritmo, del entrenamiento o de la lógica de recomendación; y sobre el operador cuando la incorrección resulte de la integración local del sistema, de bases de datos

[21] Sobre la centralidad de la supervisión humana efectiva, la transparencia y la accountability en la regulación contemporánea de la IA, véanse la Resolución del Parlamento Europeo de 16 de febrero de 2017 y el Reglamento (UE) 2024/1689.

erróneas o de la ausencia de validación exigible. Si se produce una discriminación del consumidor mediante perfilado, exclusión o tratamiento automatizado diferenciado, la responsabilidad corresponderá al proveedor si el sesgo es estructural, o al operador si la discriminación emerge de la explotación concreta del sistema en un entorno determinado.

Si existe una filtración o tratamiento ilegítimo de datos personales, la responsabilidad principal recaerá sobre el responsable del tratamiento y sobre el operador que implementa el sistema, sin perjuicio de la eventual responsabilidad del desarrollador o suministrador cuando el incidente provenga de defectos del producto o de su arquitectura. Si el sistema genera una interacción engañosa o induce al consumidor a error en la contratación, la responsabilidad deberá recaer prioritariamente sobre el operador que decide utilizarlo como interfaz de consumo y sobre el proveedor que lo comercializa sin advertir adecuadamente sus límites, sin perjuicio de la eventual cuota del mandante si utilizó dolosamente el sistema como instrumento de captación o manipulación[22].

5.5. Viabilidad y alcance de una responsabilidad autónoma del "sujeto artificial".

Conforme al estándar metodológico aquí adoptado, la eventual responsabilidad autónoma del "sujeto artificial" sólo es jurídicamente defendible como una construcción [23] legislativa futura, de personalidad derivada, funcional y finalista. Sin embargo, su justificación no se agota en la mera creación de un patrimonio separado ni en la simple adición de un nuevo deudor dentro de la cadena de consumo.

Su verdadera relevancia sistemática radica en configurarlo como un instituto especial de cierre de la responsabilidad algorítmica, destinado a dar respuesta a aquellos supuestos en los que el daño provenga de actuaciones de alta autonomía funcional no plenamente reconducibles, ex ante, ni a instrucciones específicas del mandante, ni al defecto originario del proveedor, ni a una implementación negligente del operador.

Desde esta perspectiva, el "sujeto artificial" no debe ser concebido como una ficción sustitutiva de la responsabilidad humana, sino como un centro institucional de imputación primaria provisional, de garantía patrimonial y de trazabilidad decisional, apto para absorber inicialmente la carga indemnizatoria frente a la víctima y, al mismo tiempo, permitir la posterior redistribución interna del daño mediante acciones de regreso según la fuente real de imputación. Su innovación jurídica no consistiría, por tanto, en desplazar a los actores humanos del sistema, sino en ordenar las zonas grises generadas por la autonomía funcional avanzada de ciertos sistemas inteligentes, anticipando la

[22] Guía de la AEPD destaca que la gestión del riesgo para los derechos y libertades es aplicable a todo tratamiento y que desarrolladores, encargados y suministradores pueden intervenir en esa cadena preventiva sin relevar al responsable de sus deberes propios.

[23] O. VON GIERKE, *Das deutsche Genossenschaftsrecht*, Berlin, 1887; M. HAURIOU, *La théorie de l'institution et de la fondation*, en M. HAURIOU, *Aux sources du droit. Le pouvoir, l'ordre et la liberté*, 1933; L. MICHOUD, *La théorie de la personnalité morale*, LGDJ, 1924.

tutela del consumidor y evitando supuestos de no imputación o de dispersión ineficiente de responsabilidad[24].

Por ello, el "sujeto artificial" sólo podría asumir responsabilidad propia si el ordenamiento le reconociera previamente un estatuto jurídico especial integrado, como mínimo, por identificación unívoca, domicilio jurídico cierto, patrimonio separado o fondo de garantía suficiente, seguro obligatorio o garantía financiera equivalente, registración pública, representación legal o técnica, auditorías periódicas, trazabilidad operativa integral, protocolos de ciberseguridad, monitoreo permanente de riesgos y mecanismos efectivos de suspensión, intervención o desconexión. Tales exigencias no constituyen formalidades accesorias, sino la condición dogmática indispensable para que la personalidad derivada opere como una institución de seguridad del tráfico digital y no como una máscara de irresponsabilidad.

Sólo bajo ese régimen podría sostenerse una responsabilidad primaria del "sujeto artificial" en hipótesis estrictamente delimitadas: cuando el daño derive de una decisión autónoma funcional producida dentro de su esfera operativa legalmente habilitada; cuando el sistema genere desviaciones adaptativas no imputables de modo inmediato al mandante, al proveedor o al operador; o cuando la actuación lesiva emerja de la combinación dinámica de aprendizaje, interacción y ejecución en un sistema ya registrado, solvente y jurídicamente autorizado para operar. En tales supuestos, el "sujeto artificial" funcionaría como primer patrimonio de afectación y primer centro de reconstrucción causal del evento dañoso, sin perjuicio de la ulterior determinación de responsabilidad definitiva entre los restantes intervinientes.

En otros términos, la personalidad jurídica del "sujeto artificial" no debe ser presentada como una variante sofisticada de la personificación técnica ya conocida, sino como una institución novedosa de gobernanza jurídica de la autonomía algorítmica, orientada a cumplir tres funciones indisociables: responder patrimonialmente frente a la víctima, conservar la trazabilidad relevante para la reconstrucción del daño y permitir la redistribución racional de la responsabilidad entre mandante, proveedor y operador. Es en ese triple plano – imputación, garantía y trazabilidad – donde la figura propuesta adquiere un carácter jurídicamente innovador y potencialmente singular dentro del derecho privado tecnológico.

5.6. Síntesis conclusiva.

En consecuencia, la distribución de la responsabilidad en la cadena de consumo intermediada por sistemas de inteligencia artificial debe estructurarse sobre una regla de imputación plural y jerarquizada. El mandante responde por la instrucción, la configuración decidida, la omisión de supervisión y la ratificación del exceso; el desarrollador o proveedor, por el defecto de diseño, entrenamiento, actualización, documentación o seguridad; el operador o desplegador, por la implementación concreta, la parametrización, el uso desviado, la ausencia de supervisión real y el incumplimiento de deberes de

[24] El debate europeo relativo a una eventual "electronic personhood" fue abierto por la Resolución del Parlamento Europeo de 16 de febrero de 2017, pero no fue positivizado por el AI Act, que optó por un modelo basado en riesgo, supervisión humana y obligaciones de proveedores y operadores.

información y protección de datos; y el eventual "sujeto artificial", sólo en la medida en que el legislador lo erija en una figura jurídica autónoma, de personalidad derivada, registración obligatoria, patrimonio afectado y trazabilidad integral, capaz de asumir una responsabilidad patrimonial propia, complementaria y no sustitutiva de la de los restantes actores.

Así formulada, la tesis del "sujeto artificial" no aparece como una ruptura con las bases del derecho privado, sino como una posible evolución de sus categorías de imputación frente a la complejidad algorítmica contemporánea. Su valor no reside en abstraer la responsabilidad humana, sino en contribuir, de modo técnicamente controlado, a la seguridad del tráfico digital, a la tutela del consumidor y a la protección de la libre manifestación de la voluntad en entornos tecnológicos cada vez más densos y opacos[25].

6. Internacionalización de las relaciones de consumo en entornos digitales.

Es imperativo unificar los criterios legislativos a nivel internacional en esta materia. La situación actual exige considerar al menos dos aspectos esenciales para su regulación global:

- Dada la incertidumbre en la ubicación geográfica del "sujeto artificial", lo cual restringe la posibilidad de presentar un reclamo por incumplimiento contractual y la consiguiente reparación de daños y perjuicios, se impone discutir criterios de localización jurídica, registración y cooperación internacional. Este punto conecta con la exigencia, destacada por la regulación europea reciente, de identificar con claridad a los proveedores, operadores, representantes y demás sujetos intervinientes en la cadena de valor algorítmica.
- Es fundamental implementar una regulación sobre estándares de ciberseguridad y sistemas de inteligencia artificial que garantice al consumidor y/o usuario que su uso adecuado no causará daños y perjuicios a sus bienes jurídicos. En este plano, las estrategias de privacy by design, la gestión del riesgo orientada a derechos y libertades, y la supervisión humana significativa se presentan como presupuestos normativos indispensables.

7. Conclusión.

Como conclusión provisional, considerando que este documento aborda cuestiones que, con el devenir de los acontecimientos tecnológicos, se irán ratificando o rectificando, propongo que la adecuación del derecho privado frente a la inteligencia artificial no debe consistir en una mera traslación mecánica de categorías tradicionales, sino en una reconstrucción dogmática capaz de dialogar con ellas.

[25] La finalidad última de esta construcción no es desplazar a la persona humana del centro del sistema jurídico, sino reforzar la tutela de su dignidad, su voluntad, su privacidad y su confianza frente a la creciente complejidad algorítmica.

Es imperativo que el legislador regule estas relaciones con un enfoque interdisciplinario e internacional, adaptando los contratos de mandato y consumo a las futuras interacciones jurídicas mediadas por sistemas inteligentes, pero también elaborando un estatuto jurídico específico para aquellos sistemas que, por su grado de autonomía, estabilidad funcional y aptitud para incidir en el tráfico, requieran una disciplina singular.

Además, resulta esencial establecer estándares claros de ciberseguridad, transparencia, trazabilidad, auditoría y responsabilidad para garantizar que el uso adecuado de la inteligencia artificial no provoque daños. Por consiguiente, la creación del "sujeto artificial" debe ser presentada como una propuesta de lege ferenda: compatible con la tradición de la personalidad jurídica, pero distinta del derecho positivo actual de la Unión Europea, que en el AI Act prefirió un modelo regulatorio basado en el riesgo y en obligaciones para actores humanos e institucionales, y cabe agregar que su valor no radica únicamente en responder, sino en ordenar la responsabilidad algorítmica compleja.

Independientemente de lo hasta aquí expresado, es fundamental no perder de vista la importancia de esta propuesta regulatoria, cuyo objetivo principal es proteger la libre manifestación de la voluntad humana. El debate europeo sobre una eventual "personalidad electrónica", abierto por la Resolución del Parlamento Europeo de 16 de febrero de 2017, muestra que la cuestión ya ha sido advertida; pero el hecho de que el AI Act no haya consagrado esa solución no clausura la discusión, sino que obliga a replantearla con mayor rigor dogmático. La tesis aquí sostenida no procura desplazar a la persona humana del centro del sistema jurídico[26], sino precisamente preservarla frente a la creciente complejidad algorítmica. En esa línea, la distribución de la responsabilidad debe responder a un criterio plural y jerarquizado, atendiendo a la instrucción, al defecto de diseño, a la implementación concreta y, sólo de lege ferenda, a la eventual actuación patrimonialmente imputable del "sujeto artificial".

[26] J. C. PALMERO, *La persona jurídica en el proyecto de unificación de la legislación civil y comercial de la nación*, en *Revista del Derecho Comercial y de las Obligaciones*, 20, 1987, 817–835.

Gatt L, 'Instances of legal subjectivity between the natural and artificial worlds: the new content of the legal subjectivity of the natural human being in a perspective of protection of vulnerability as the authentic content of sustainability' (2025) 2 EJPLT
DOI: https://doi.org/10.57230/EJPLT252LG

EJPLT
ISSN 2704-8012

Instances of legal subjectivity between the natural and artificial worlds: the new content of the legal subjectivity of the natural human being in a perspective of protection of vulnerability as the authentic content of sustainability

Istanze di soggettività giuridica tra mondo naturale e artificiale: il nuovo contenuto della soggettività giuridica dell'essere umano naturale in una prospettiva di tutela della vulnerabilità come autentico fondamento della sostenibilità

LUCILLA GATT
Full Professor of Civil Law and New Technology Law
Director of the JM Centre of Excellence – ReCEPL4STAI
Università degli Studi Suor Orsola Benincasa

Abstract

This article addresses the issue of legal subjectivity, arguing for its expansion. Although human beings have always been regarded as the quintessential subjects of law, recent legal developments in Europe are challenging this anthropocentric perspective, promoting a growing recognition of various forms of vulnerability and their legal protection. Thus, a transition is emerging toward a conception of legal subjectivity in terms of responsibility toward vulnerable living beings, which could extend beyond human beings and reflect a significant cultural and social shift.

Il presente contributo affronta il tema della soggettività giuridica, sostenendone l'espansione. Sebbene gli esseri umani siano sempre stati considerati i soggetti del diritto per eccellenza, i recenti sviluppi giuridici in Europa stanno mettendo in discussione questa prospettiva antropocentrica, promuovendo un crescente riconoscimento delle varie vulnerabilità e della loro protezione giuridica. Si profila così una transizione verso una concezione della soggettività giuridica in termini di responsabilità verso i viventi vulnerabili, che potrebbe estendersi oltre gli esseri umani e riflettere un significativo cambiamento culturale e sociale.

* Il presente lavoro è un ampliamento e una traduzione in inglese del contributo pubblicato in lingua italiana nel volume M. Pittalis (a cura di), *Diritto degli esseri animali. Dibattito* (Cacucci, 2025), pp. 51-66. This work is an expansion and an English translation of the contribution published in Italian in the volume M. Pittalis (ed.), *Diritto degli essere animali. Dibattito* (Cacucci 2025) pp. 51-66.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Commons Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the licence are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: legal subjectivity; legal personality; legal responsibility; new category; vulnerability; sustainability; animals; plants; human beings; vegetarianism; medical experimentation; hunting

Summary: 1. The traditional conception of legal subjectivity. – 2. Signs of change: regulatory developments in Europe. – 3. Changes in the content of legal subjectivity: the relationship between vulnerability and environmental sustainability. – 4. The legal subjectivity of natural and legal persons, both public and private: from domination to the protection/care/safeguarding of vulnerable beings. – 5. Obstacles to the change in legal subjectivity in terms of the tutoral responsibility of human beings towards other living beings. – 6. Implications of the new category of legal subjectivity for the category of sustainability: vegetarianism and alternative medical experimentation. – 7. Conclusions.

1. The traditional concept of legal subjectivity.

The current civil code is rooted in the dichotomy between subject and object of law. This dichotomy is the culmination of a long journey that began with the Declarations of the 18th century and continued with the continental codifications of the 19th and 20th centuries, leading human beings to place themselves at the centre of the natural and legal world as subjects of law.

At the present moment in history, human beings are considered in the legal systems of the Western cultural area to be the subject of law par excellence, identified with the natural person without further qualification. Alongside the natural person as a subject of law, the legal person was created at the beginning of the 19th century by Heise and von Savigny (and in the wake of the canonistic tradition) as a subject of law that exists only in the reality and language of law. It is the result of the conceptual apparatus of law, which has literally invented and made legally relevant a subject that is different from the natural person: the legal person is a non-tangible subject that exists only in the legal world, unlike natural persons, who also exist in the natural world.[1]

In other words, law has historically demonstrated its ability to «take away and give», to attribute or not attribute the status of legal subject to the same natural persons, considering them different from one another for various reasons (race, sex, religion). To date, legal subjectivity – understood as the recognition of full accountability for rights and duties – is not attributed in the same way throughout the world, and there are still very significant differences.

There were differences in legal subjectivity between free individuals and slaves; there were and still are differences in some areas of the world between men and women, but also between believers of one religion and believers of another, and even between migrants from different countries. During Nazism, in the middle of the 20th century, and despite codification, some European legal systems deprived members of the Jewish population of legal subjectivity,

[1] E Gliozzi, 'Persona giuridica', *Enciclopedia delle Scienze Sociali* (1996) <https://www.treccani.it/enciclopedia> accessed 15 july 2025.

rendering them '*res*', but, as recent wars covered by the Western media have shown, forms of non-recognition of full legal subjectivity for human beings still emerge.

The historical perspective shows that legal subjectivity is an artificial *status*, a *status* that can be attributed or withdrawn in relation to the social, political and economic contingencies of a given legal system. Within a certain territory where certain rules apply and there is a power capable of enforcing them, it is possible to decide to attribute legal subjectivity to some subjects rather than others.

There are currently at least 18 conventions on fundamental human rights, from which it can be deduced that human beings are undoubtedly the subjects of law par excellence in legal systems (Western but not only).

However, far from being a point of arrival, this state of affairs is currently the subject of heated debate. There is a clear transition towards something else and, more precisely, towards the recognition of other legal subjects or even towards the recognition of a different legal subjectivity of human beings.

From a cultural, social, economic and therefore also legal point of view, there is a rethinking of the category of legal subjectivity as attributed exclusively to human beings as physical persons. This is a general rethinking because the relationship between human beings as physical persons and their surroundings (i.e. the natural world but also the artificial world, the world of machines, software and technology that creates non-natural entities) is changing. As a result of this progressive change in the relationship between human beings and the natural world and between human beings and the artificial world, the category of legal subjectivity is also changing. There is intense debate in academic circles about who, other than human beings, can be a subject of law, but there is also debate about the content of legal subjectivity, as it is (finally) being recognised that this content cannot consist exclusively in the ownership of rights over other natural and artificial entities.

The relationship between human beings and the natural world has been well summarised in the 43rd edition (2007) of Alberto Trabucchi's *Istituzioni di diritto civile* (Institutions of Civil Law, a classic work of civil law literature), where we read on page 527: *«by supreme law, man was subjected to the dominion of the external world»* (our translation). These statements can be found, in a more or less explicit form, throughout Italian private law textbooks, particularly since the 2000s (i.e., recently). These textbooks express the idea that the human being as a physical person is the subject to whom all possible rights are attributed, the one who can exercise them, a ruler, a subject who has dominion over the external world, which he can shape, modify, use and even destroy. This is because the concept of dominion also includes – as attested by the legal institution of property – a destructive power and not only a power of control or management.[2] The idea of dominating, controlling and potentially destroying (everything that is not human) is inherent in the concept of the human being as a subject of law as regulated by the rules of the civil code and described in private law textbooks.

[2] J Mason, *Un mondo sbagliato. Storia della distruzione della natura, degli animali, e dell'umanità*, trans. Massimo Filippi (Sonda 2015) 46 ff. and more recently the same Author has published *An Unnatural Order. The Roots of Our Destruction of Nature* (Lantern Publishing & Media 2021).

Western legal culture is therefore based on the ideology of domination and an anthropocentric conception of human beings, even though the phase of attributing legal subjectivity to some human beings at the expense of others has been overcome (a phase that is still ongoing in other legal systems). This overcoming leads to the denial – at least formally – of any legitimacy of the prevalence of some human beings over others, considered different or, rather, inferior for various reasons.

Italy (but one could say Europe) fits perfectly into this legal framework of the permanence of the ideology of domination with regard to the 'human-nature' relationship and the overcoming of this ideology with regard to the 'relationship between human beings'. The ideology of domination manifests itself in the structuring of the categories of subject and object of law and informs the institution of private property and power.

The Civil Code remains the main source of rules governing relations between legal subjects considered to be in an equal position, i.e. involved in private law relationships. In this context, the rules that most emphasise the dichotomy between subjects and objects of law are: Articles 1 and 5 (concerning the human body), Articles 11 to 14, Article 810, Article 842, and Article 923 of the Civil Code.

Article 810 of the Civil Code is important because it states that *«things that can be the subject of rights are property*» (our translation). In other words, all *things* that are the subject of law are *property*. Clearly, the subject of law who is the holder of the rights exercised over objects is excluded, and this subject of law is the human being (and, as mentioned, from a certain point in history onwards, it is also the legal person). The current validity of this article and its content unequivocally attests that human beings persist in the belief that they are essentially the rulers of the world and have granted legal personality to intangible entities such as legal persons because they act through natural persons[3] .

Animals are clearly indicated in the main private laws, and in Italian law in particular, as objects of law. Article 842 of the Civil Code, entitled *'Hunting and* fishing' (our translation), states: *«The owner of land may not prevent anyone from entering it for the purpose of hunting, unless the land is closed in the manner established by the law on hunting or there are crops in progress that are susceptible to damage. He may always oppose anyone who does not have a licence issued by the authority. The consent of the owner of the land is required for fishing»* (our translation).

It is clear from the text that hunting is an activity inextricably linked to *the ownership* of land and that anyone may engage in it. Article 923 of the Italian Civil Code is along the same lines, stating that: «*Movable property that is not owned by any r is acquired by occupation. Such property includes abandoned items and animals that are the object of hunting or fishing»* (our tranlsation).

Starting from these unequivocal regulatory provisions, ownership, as the structural modus operandi of the subject of law, has been greatly extended thanks to the broadening of the concept of property. The idea of property has developed and expanded, as has been clearly highlighted by the best civil law

[3] Gatt L, 'Commento all'art. 810 c.c.' in L. Gatt and S. Troiano (eds.), *Commentario al Libro III del Codice Civile*, directed by C.M. Bianca (Dike Giuridica 2014).

doctrine, which has emphasised the need to consider as property in the legal sense «*any legally relevant material or immaterial entity*».[4]

Therefore, while the category of legal subject remains limited to natural persons, since the enactment of the Civil Code in Italy (and, in general, in Western legal culture), the concept of property, *i.e.* the object of law, has expanded enormously. This extension has broadened the domain of human beings, and in this enormous and uncontrolled expansion, all non-human living beings are perceived as things to be used and/or transformed.

In particular, with regard to animals, we have witnessed and continue to witness 'metamorphoses' that are considered entirely legitimate: animals (but also other living beings) are transformed into food, clothing, entertainment, sport, research and teaching tools.[5] In almost all cases, this transformation results in the painful death of non-human living beings, their decimation, and often their definitive disappearance as a species, but in the logic of absolute and legitimate human domination, this does not represent a problem either in terms of private law or constitutional law. If, in fact, animals – as mentioned – appear in codified texts, albeit as objects of law, they are completely absent from texts in the broad constitutional sense and, in any case, from bills of rights, which remain [rights] human and only human.

2. Signs of change: regulatory developments in Europe.

This scenario in Europe remained completely unchanged until the end of the 1980s, when it began to change in the last two decades of the 20th century and underwent a rapid and crucial change in the first decade of the 21st century. The idea of the human being as the sole subject of law, the sole ruler, the holder and exerciser of rights over all other goods, *i.e.* over all other entities, living and non-living, material and immaterial, identifiable (not only on planet Earth, consider all the issues that arise regarding the colonisation of extra-atmospheric and extra-planetary space), there are different views in many European (and, above all, non-European) countries.

To briefly summarise some of the most significant milestones, it should be noted that in Austria, the process of 'dereification' of animals began as early as 1988[6] with the introduction of paragraph 285a of the ABGB, which states that animals are not things and are protected by special laws; the provisions applicable to things are valid only in the absence of contrary provisions. Subsequently, with Federal Constitutional Law No. 111/2013, Preamble §2, Austria undertook to guarantee the welfare of animals by introducing the concepts of sustainability, including with regard to research, global environmental protection and the guarantee of a healthy environment, as §2, Austria undertook to guarantee animal welfare, introducing the concepts of sustainability, including with regard to research, global environmental

[4] CM Bianca, *Diritto civile VI*, *La proprietà* (Giuffrè 2017) 33 ff.
[5] T Regan, *Gabbie vuote. La sfida dei diritti degli animali*, trans. M Filippi and A Galbiati with L Zonca in collaboration (Sonda 2009)
[6] D Franco Silva, 'Gli animali non sono cose: significato di un'affermazione' in MC De Cicco (ed), *Annali della Facoltà Giuridica dell'Università di Camerino, No 8/2019* (Università di Camerino Faculty of Law 2019).

protection and the guarantee of water and food supplies as fundamental principles of the Austrian legal system, thus completing the process begun with the Federal Animal Protection Act (Tierschutzgesetz – TSchG) of 2004.

In Germany, paragraph 90 was introduced into the BGB in 1990, reproducing the content of the provision of the Austrian Civil Code. However, Germany was ahead of Austria, as animal protection had already been enshrined in the constitution in 2002 with paragraph 20a of the *BundesGesetz*, according to which the state assumes responsibility for protecting the natural foundations of life and animals as its duty to future generations.

At European level, in 2007, the Treaty of Lisbon brought about an important change with the introduction of Article 13 into the consolidated version of the Treaty on the Functioning of the EU (TFEU), which states that both the Union and individual Member States, when acting in certain areas, must take into account the well-being of animals as sentient beings. This definition represents a step forward in the process of *dereifying* animals, although it cannot be considered a point of arrival. On the other hand, it should be emphasised that the above-mentioned national measures predate it and are not subsequent to it. With the exception of the Netherlands, where there have been no constitutional measures but only amendments to the Civil Code since 2011, when Article 2a of Book III of the BW was introduced, recognising animals as having a status different from that of objects but specifying that they are subject to the legal regime of *res,* in compliance with legal limits, obligations and principles based on statutory rules, unwritten law, public order and morality.

France remains resistant and, only several years after the Treaty of Lisbon, began a process of reflection that led in 2015 to an amendment to Article 514-15 of the Civil Code in order to define animals as «*living beings endowed with sensitivity*», while continuing to consider them as objects of law (*Les animaux sont des êtres vivants doués de sensibilité. Sous réserve des lois qui les protègent, les animaux sont soumis au régime des biens)*.

The Swiss legal system appears more advanced, where in 1999, under Article 80 of the Federal Constitution, the Confederation issued regulations on *the protection* of animals, specifically governing: «*their keeping and care; experimentation and any procedure conducted on live animals; the use of animals; the importation of animals and products of animal origin; the trade, transport and killing of animals*» (our translation). It should be noted that the cantons are responsible for ensuring the application of the laws on this subject, unless this competence is otherwise reserved to the Confederation, which is always competent to legislate on the use of genetic and productive material of animal origin, but must do so taking into account the dignity of living beings and the safety of humans, animals and the environment, protecting the genetic diversity of the plant and animal kingdoms (see Article 120 of the Federal Constitution). Through this constitutional provision, the Swiss legal system, more than other legal systems in the Western, is moving towards equal consideration of humans and animals, but above all it is taking into account an area that is currently undergoing enormous expansion due to the development of biotechnology, namely that of human-animal hybridisation aimed – mainly but not exclusively – at xenotransplantation.

In Italy, it was only at the beginning of the 21st century that the position of absolute domination of humans over animals began to crack. With Law 189/2004, Title IX-bis was added to the Penal Code concerning 'crimes against animal welfare' (Articles 544*bis*-544*sexies* of the Penal Code); Article 727 on the abandonment of animals was also amended, providing for severe penalties for those who abandon domestic animals. These are important measures in terms of instruments in favour of mistreated animals, although they are not yet decisive at a conceptual level, as they are still anthropocentric in nature, given that the protected good is man's feelings towards animals and not the animals themselves. The wind of change has not even touched the rules governing condominiums (Article 1138 of the Civil Code, as supplemented by Law No. 220/2012), which are also aimed at protecting the owners rather than the animals.

For a long time, nothing changed and the above-mentioned provisions remained unchanged until 2022. When read in conjunction, they unequivocally confirm that, in the Italian legal system, animals are classified as objects of law, without any overlap with the category of subjects from a legal perspective. Even the recent Constitutional Law No. 1/2022 does not formally affect the classification of animals as objects of law: the amendments to Articles 9 and 41 of the Constitution have specified that animals must be protected. In doing so, the constitutional law confirmed their legal nature as objects of law but removed them from the broad category of objects for which there are no protection obligations.

Not only that: the inclusion of a constitutional obligation to protect animals affects the content of the legal subjectivity of human beings. It does not therefore seem inappropriate to consider that, thanks to Constitutional Law No. 1/2022, the ideology of human domination over nature and animals has come to an end in our legal system, at least as far as the founding legal texts are concerned, and that the transformation of the legal concept of legal subjectivity has begun, even in our country.

3. Changes in the content of legal subjectivity: the relationship between vulnerability and the category of environmental sustainability.

Since the end of the first decade of the 21st century, the surge in technological development, climate and environmental emergencies, the launch of the Green Deal and the cascade of regulations from the European Union since the beginning of 2020 have led to an unstoppable transformation of the traditional dialectic between the subject and object of law, generating a new vision of the possible relationship between man and nature and configuring it no longer in terms of absolute domination but in terms of vulnerability.

The word 'vulnerability' (from the Latin '*vulnerare*', to wound) literally means «likely to be wounded». In a figurative sense, it refers to the precariousness of a condition characterised by the possibility of violation and limitation, often defined by varying degrees of weakness, dependence and lack of protection. The 1998 "Barcelona Declaration" represents an important event in the

recognition of vulnerability as a category in view of its possible public legitimisation.

The Declaration is the result of a three-year discussion between 1995 and 1998, undertaken by a group of 22 partners from different countries within the enlarged European Community and coordinated by the Danish Centre for Ethics and Law in Nature and Society (Copenhagen).

It is often better known as 'The Barcelona Declaration on Policy Proposals to the European Commission on Basic Ethical Principles in Bioethics and Biolaw'. It was a broad, multi-level discussion involving educators, researchers, professionals and, above all, European citizens.

The public debate was summarised in two large volumes (Basic Ethical Principles in European Bioethics and Biolaw vol I; Basic Ethical Principles in European Bioethics and Biolaw vol II) and led to the formulation of four principles of autonomy, dignity, integrity and vulnerability, known as the Barcelona Declaration, which were presented to the European Commission as a summary of the basic ethical principles underpinning the European community.

In the legal sphere, vulnerability is a relational concept in that it manifests itself and takes concrete form in the possible relationship between two entities.[7] It is a multidimensional and interrelated condition that is no longer a status linked to old age, minority, female gender or disability. In the current national and international legal framework, vulnerability has acquired a broader meaning that includes all living entities, from humans to animals or plants, when they operate in contexts – such as industrialised ones – where other actors (humans) are more powerful for various reasons: social, economic or cultural, physical strength, possession of weapons and, last but not least, the technological gap. A relationship of vulnerability arises when there is an imbalance in the starting positions, which determines the vulnerability of one living entity towards another living entity. This condition, in turn, means that one living entity is able to profit at the expense of another living entity or, more dramatically, to cause it pain or death.

On closer inspection, therefore, there are many relationships that can generate conditions of vulnerability; not only that between human beings and nature, but also that between men and women, adults and minors, white men and black men, Catholics and Muslims, indigenous peoples and colonisers, and so on.

Having identified the relationship of vulnerability in these terms, it seems plausible to assert that: 1) the abuse of a human being in a position of greater power/strength to the detriment of another living being is unjust, i.e. ethically unacceptable; 2) the entity in a position of greater weakness – i.e. the vulnerable entity – must be protected from any abuse of power/force by the stronger entity.[8]

From a historical perspective, therefore, it appears that Europe has long based its development on the concept of vulnerability. However, it is only

[7] L Gatt, 'Legal anthropocentrism between nature and technology: the new vulnerability of human beings' (2022) 1 EJPLT 15–26.

[8] L Gatt and IA Caggiano, 'Consumers and Digital Environments as a Structural Vulnerability Relationship' (2022) 2 EJPLT 8–16.

recently that a real awareness of what this choice means and, above all, of the consequences it has in terms of its application in the economic and legal spheres, has been gaining ground in European governance.

In other words, it is only relatively recently that the idea has penetrated Western European culture that greater physical, intellectual, cultural and economic strength does not entitle those who possess it to oppress in various ways those who cannot react with equal force.[9]

Only recently we have seen political choices and the enactment of legislation that reflect the idea that a position of greater strength translates into greater responsibility towards those who find themselves in a different position, i.e. one of weakness and subordination. This trend can be observed in European and non-European policies on the Green Deal and human-centred Artificial Intelligence (where the potential of these approaches is considered and they are not seen as mere expressions of law-washing).[10]

This trend has certainly been driven by the advancement of sustainability, which is itself a consequence of greater awareness of the impact of the ideology of human domination over nature: climate change, depletion of energy resources, extinction of animal and plant species, extinction or ghettoisation of indigenous peoples, reduction of dedicated spaces (think of the ongoing battle in Brazil to prevent deforestation and the seizure of territories from indigenous peoples, in addition to similar battles in Uganda, etc.)[11]. The destructive force inherent in the exercise of domination by the human legal subject has taken on a self-destructive dimension that has generated changes of course, reflections and demands for change.

This attests to an evolution in European culture (not only legal) of the concept of vulnerability in the sense of a transition of the vulnerable entity (*i.e.* the weaker entity) from an object of oppression or, in any case, of unconditional exploitation to a subject to be protected. That said, the tools that can be used to combat abuse and protect vulnerable subjects from abuse are preventive or repressive in nature. In both cases, the law comes into play, i.e. a mandatory regulatory framework with adequate provisions and corrective measures. These rules make abuse of vulnerable living beings unlawful, abuse that would otherwise be merely ethically unacceptable (unjust and, therefore, left to

[9] U Mattei, L Nader, *"Plunder". When the Rule of Law is Illegal* (Blackwell 2008) (Italian version: U Mattei and L Nader, *Il saccheggio. Regime di legalità e trasformazioni globali* (Mondadori 2010)).

[10] CODEX Conference - Ideologies and Techniques of the (re)codification of Private Law, 15-17 March 2018, carried out as part of 'Legacy,' i.e., the framework of study dedicated to the memory of Stefano Rodotà, organized by the International University College (of which Rodotà was president from 2008 to 2014) and the Collegio Carlo Alberto at the new headquarters of the University of Turin, under the supervision of prof. Ugo Mattei. Codex will be followed by Civitas, an in-depth study dedicated to the city between social public goods and common goods, according to the well-known taxonomy of the Rodotà Commission. See the Conference brochure to the link <https://www.dirittieistituzioniphd.unito.it/avvisi/att/121h.allegato.pdf> The conference proceedings collection is available at this link: U Mattei (ed.), *Codex: Ideologie e Tecniche della (Ri) Codificazione del Diritto Privato* (2019) 25(1) The Cardozo Electronic Law Bulletin Review (free pdf: <https://www.academia.edu/40702536/Vol_25_1_Spring_Summer_2019_Codex_Ideologie_e_Tecniche_della_Ri_Codificazione_del_Diritto_Privato>).

[11] D Lema, A Vasquez, 'Forced Displacement of Indigenous Peoples in the Amazon Caused by Environmental Hardship: a Case for Human Security' (2022) PHRG 6(2), 159-180; M Mantovani, 'Cop della Foresta: l'Amazzonia tra tutela, sfruttamento e diritti indigeni' VALORI. <https://valori.it/cop-foresta-amazzonia-popoli-indigeni/>.

individual conscience, as is still largely the case today, given that this change in the content of legal subjectivity is still in progress).

From the perspective of regulatory interventions aimed at protecting vulnerability, specifically in relation to the relationship between humans and nature, we believe that the 2022 amendment to Article 9 of the Italian Constitution clearly represents the path to follow. The Constitutional Charter, in its original formulation, marked the overcoming of numerous conditions of vulnerability (those between genders, between followers of different religions, between human races, social classes, etc.). However, animals were not included, nor was the condition of human-nature vulnerability, and the constitutional law has filled this gap. The difficult journey of implementing this provision and its application at various levels now remains.[12]

4. The legal subjectivity of natural and legal persons, both public and private: from domination to the protection/care/safeguarding of vulnerable beings.

With the 2022 intervention, with the Italian State expressly assuming an obligation to protect the environment, biodiversity and ecosystems, also in the interests of future generations and animals, an important step forward has been taken towards overcoming the traditional content of the two dichotomous terms of subject and object of law. On an ideological and technical-legal level, the State has clearly stated its intention to protect animals, to protect them uniformly and well.[13]

The relationship of domination is beginning to crumble as the terms 'safeguard' and 'protect' gain ground: the Italian State has a duty to become an entity that protects weaker entities, a guardian, a caretaker, and must be vigilant. This obligation incumbent on the Italian State also falls on all Italian citizens, on every natural person, on every Italian human being who is a subject of law.

This obligation corresponds to rights in favour of the entities referred to in Article 9 of the Constitution. It should be noted, however, that legal subjectivity is not attributed to animals, just as it is not attributed to the environment, biodiversity, ecosystems or future generations. What has happened in other countries (Ecuador, Bolivia, Argentina, India), where legal subjectivity has been attributed to animals and natural entities,[14] has not happened in Italy. There is no doubt that at this moment in history, the legal and religious cultures of other areas of the planet (Latin America, India, Asia) are expressing advanced visions of a revision of the relationship between humans and nature, or more precisely, a formal and legal (re)affirmation of a conception that is profoundly different from that of Western cultures: respect and harmony between humans and the

[12] L Gatt, 'Evolution of legal subjectivity as private law category in the new Italian Constitution' in F Rescigno and D Cerini (eds.), *Sustainability and animal welfare: legal and scientific perspective* (Routlegde-Giappichelli Studies in Law 2025) 35-47.

[13] F Rescigno, 'La riforma dell'articolo 9 e gli esseri animali: un impegno verso una Costituzione biocentrica e animalista' in *One Earth – One Health. La costruzione giuridica del Terzo Millennio* (Giappichelli 2023) 13–21.

[14] M Pittalis, *Diritto degli esseri animali – Lezioni e commenti* (Cacucci Editore 2022).

natural world are cardinal concepts of the religions and cultures of many Latin American, Asian and Indian peoples.[15]

However, the failure to attribute legal subjectivity in our constitutional text does not seem to represent an obstacle to the changes taking place and, indeed, is itself a manifestation of the change that has taken place in , as it attests that the Italian State and Italian citizens, while remaining exclusive subjects of law, no longer have a position of dominance over nature and animals, but must, on the contrary, protect them.

In other words, attributing legal subjectivity to animals is not the solution to the problem of their vulnerability unless the very content of legal subjectivity as it relates to human beings is changed. The content must be one of care and protection towards the weak (animals, but also the environment, the plant world, biodiversity, etc.). By attributing this content to the legal subjectivity of legal persons and human beings in relationships of vulnerability, we see how the state and human beings become responsible towards all animals and, in general, towards all living beings that are unable to protect themselves autonomously.

The Italian constitutional reform has initiated this process; slowly, the awareness is emerging that being subjects of law does not mean being rulers but guardians; it means being those who must protect, preserve and avoid abusing everything that does not have the possibility of defending itself, protecting itself and protecting itself autonomously. A different concept of legal subjectivity is emerging, one that is more about duties and responsibilities than rights and powers, because this concept of legal subjectivity is becoming increasingly rich in elements of necessary relationality with what surrounds human beings, in particular with other living beings.

The Italian legal system is no stranger to these changes in the meaning and content of active legal positions. With regard to another topical relationship of vulnerability, that between minors and adults, the 2012-2014 family law reform replaced parental authority with parental responsibility (Article 316 of the Civil Code). This type of active legal position is full of duties and much less of rights, *i.e.* of powers of the adult towards the minor. On the contrary, the position of the minor is rich in rights and has very few duties.

A similar position should be taken by human beings towards nature, animals and plants: one could speak of tutorial responsibility.

The transformation of the content of legal subjectivity in relation to human beings also involves the legal personality of entities, especially states but also private entities. All legal subjects – natural and legal persons – are now called upon to exercise the powers connected with their legal subjectivity in the spirit of care and protection of non-human living beings.

[15] MC Gaeta, 'Il problema della tutela giuridica della natura: un'analisi comparata tra Italia e Stati dell'America Latina' (2020) 4 NDC 313–343.

5. Obstacles to the change in legal subjectivity in terms of the tutoral responsibility of human beings towards other living beings.

Against this process of profound change in the content of legal subjectivity, whether it refers to natural or legal persons interacting in contexts of relational vulnerability, there is a certain type of technological development that promotes, instead, the traditional dualism of legal subjectivity-autonomy, the latter understood as intellectual capacity and/or awareness/responsibility for one's actions, and supporting the attribution of legal subjecthood only to entities that possess it.[16]

These currents of thought, which are widespread internationally and combine moral philosophy, law and bioethics, at best endorse the extension of legal subjectivity to animals as a useful argument for extending it to autonomous artificial agents (robots in the broad sense) and to the environment.

Despite their good intentions, these schools of thought, anchored in the traditional conception of legal subjectivity, prevent the recognition of the content of care for non-human living beings; they prevent the development of an idea of protection and safeguarding that human beings should have towards other living beings, and instead push towards the attribution of legal subjectivity – traditionally considered exclusive to humans – to anthropomorphic robots.[17] Remaining closed within this conceptual bubble, it becomes difficult to understand that attributing legal subjectivity to robots should not mean making these artificial agents dominators of humanity and nature. On the contrary, it should mean programming them so that they can exercise care and protection of human beings and non-human living beings and also make them responsible for any damage caused to them. In other words, robots as legal subjects should be understood as entities obliged to protect and safeguard all living beings, and this could be relatively easy to achieve at the design stage if only this objective were clear.

While waiting for this perspective to take hold (which seems to be moving further away with the creation and widespread use of so-called weapon robots), the more 'progressive' currents are seeking to justify various forms of reification of human beings themselves, as well as non-human living beings.

In particular, the advance of biotechnology is cause for concern. This advance requires the use of all living beings, from humans to plants and animals, for specific purposes. Paradoxically, alongside the above-mentioned trends towards expansion or, in any case, transformative enlargement of the category of legal subjectivity, we are witnessing a simultaneous shift of all living beings, including human beings, particularly in their embryonic forms, towards the category of legal objects. This is happening with the use of biotechnology in the broadest sense: gene editing; human-animal hybridisation techniques; incubation and artificial procreation of triparental embryos and, above all, synthetic human embryos (Sheefs - Synthetic Human Entities Embryo-Like Features).

---

[16] JC Gellers, *Rights for Robots: Artificial Intelligence, Animal and Environmental Law* (Routledge 2021).
[17] L Gatt, 'Legal anthropocentrism between nature and technology: the new vulnerability of human beings' (2022) 1 EJPLT 15–26.

It is clear that this scenario greatly slows down the development of legal subjectivity for persons (natural and legal, and why not robots equipped with AI) towards the care and protection of vulnerable living beings (including human beings).

On the contrary, in the aforementioned scenario, the idea of a human being who is still dominant for purposes (medical research; advancement of medical care; scientific progress, etc.) that he himself has placed above his obligations to protect even entities of his own species (human, in fact) is endorsed.[18]

In other words, technology, insofar as it places human beings in a position of absolute supremacy not only over other living beings but also over other humans (in their various stages of development), can represent and has so far represented an obstacle to the acceleration of the conceptual metamorphosis of the relationship between humans and nature, which is nevertheless evolving, albeit slowly but surely.[19]

From a different perspective, it must be said that this trend could well be reversed, making technological development a powerful ally in the decline of legal subjectivity in the sense of care and protection of living beings in vulnerable positions.[20]

6. The impact of the new category of legal subjectivity as care on the category of sustainability: vegetarianism and alternative medical experimentation.

The reversal of the trend regarding the possible uses of technological development is, in reality, already underway because there are regulatory data and technological discoveries of fundamental importance in Europe that allow us to take a clear and perhaps even rapid direction towards the effective sustainability of humankind on the planet.

The issue of sustainability cannot be reduced to a more or less rational attempt to hoard new sources of energy (perhaps at the cost of destroying other living beings) with the main, if not exclusive, aim of preserving the current lifestyle of Western people. This would ignore the deep link between sustainability and vulnerability, which is the core concept on which the new way of being and thinking of the next generations should be based.

Promoting a culture of sustainability means promoting a culture of relational vulnerability and the repositioning of human beings in relation to nature, natural environments, ecosystems and habitats that are home to animals, plants (but also humans who are culturally, economically, militarily and technologically weak).[21]

---

[18] AG Biuso, 'Biotecnologie e antropodecentrismo' in L De Stefano (ed), *Tecnica e Coesistenza: Prospettive antropologiche, fenomenologiche ed etiche* (Mimesis 2024) 149–156.

[19] L Gatt, 'Essere umano e ambiente digitale come relazione di strutturale vulnerabilità' in L. Gatt and M.C. Gaeta (eds), *Building a New Strategy for European Protection Law in a Technological Environment* (Suor Orsola Benincasa University Press 2023) 11 ff.

[20] This concept also includes the human embryo in all its forms, see P Grimaldi, End of Waste (EoW) nell'attività di impresa tra sostenibilità, artificial intelligence e digital innovation (Suor Orsola Benincasa University Press 2024) 106.

[21] L Gatt, 'Il paradigma della sostenibilità nel diritto privato tra vulnerabilità relazionale e "principio responsabilità' in I.A. Caggiano and A.A. Mollo (eds), *Eu Green Rights: re-shaping fundamental rights for future*

The repositioning of human beings in the role of guardians of those who can only suffer without being able to defend themselves requires, first and foremost, the recognition and codification of:

a) the right of animals not to be killed for pleasure (abolition of all forms of use of animals for recreational and sporting purposes, even if long-standing in all its forms and in all countries of the world);

b) the right of animals not to be eaten in a serial and industrial manner or for religious reasons that often fuel the serial and industrial way of animal exploitation for food;[22]

c) the right of animals not to be subjected to medical experimentation (with or without vivisection).

These three rights and the related obligations incumbent upon public legal entities – states – and private entities, as well as upon human beings as such and as citizens – appear fundamental and indispensable: their recognition is a *sine qua non* condition for the repositioning of human beings and for the change in meaning and content of the category of legal subjectivity.

It follows that the promotion of vegetarianism and alternative techniques to animal experimentation must be the main objectives of technological development with a view to real sustainability.

It should be noted that we have actually been making good progress in this area for some time.

Consider the possibility of using robot animals to satisfy recreational and sporting needs for violent human-animal interaction.[23]

Consider cultured meat as a means of eliminating livestock farming. Cultured (or, erroneously, synthetic) meat was discovered in the 1970s and is already on the market in Asia (Singapore, South Korea) and will soon be available in other parts of the world.[24] The importance of this 'technology' has also been highlighted by P. Benanti.[25] Inexplicably, in Europe, various excuses

---

*generations. La sostenibilità nella prospettiva europea dei diritt*i, ReCEPL Series (Suor Orsola Università Editrice, 2025) vol. 8 15-29; L Gatt and others, 'Vulnerabilità tecnologica: una prospettiva di diritto privato' in A Patroni Griffi (ed.) *Vulnerabili. Questioni giuridiche, dilemmi bioetici*, (Mimesis 2025), 611-655; AA Mollo, 'Vulnerabilità e sostenibilità: primi spunti per uno studio dell'impatto sulle persone con disabilità e sulle future generazioni dei dispositivi [neuro]tecnologici' (2023) Special Issue EJPLT 28–40.

[22] We wish to counter the common objection that the killing of animals in agricultural, rural and similar contexts is legitimate, by arguing that such contexts are fundamentally different from those mentioned in the text, where there is a complete lack of balance between the interests of humans and those of animals: in the food industry, in fact, humans totally exploit animals in order to excessively satisfy their own dietary needs (with negative consequences even for their own health).

[23] A mechanical bull is a machine designed to replicate the motion of a bucking bull. Originally developed for training rodeo riders, it lets people practice without the danger or harm to live animals. Today it's widely used as entertainment or competitive amusement in bars, fairs, and events. This is one of the clearest examples of a robotic substitute for a violent human–animal sport (bull riding). Experimental robot bulls (bullfighting alternatives) There have been prototypes like an autonomous bullfighting robot ("robot bull") designed to mimic the behavior of a bull in corrida-style scenarios. These are not mainstream yet but illustrate attempts to replace bullfighting with safe robotic simulators. Robotic "animal-like" systems used in competitive or aggressive sport contexts: Robot combat / robot "fighting sports". Robot competitions include: Robot combat (machines fighting each other); Android wrestling / boxing; "Creature-style" robots in combat arenas [topendsports.com], [youtube.com]. Events like the World Humanoid Robot Games include: kickboxing; contact sports [smithsonianmag.com]. These replace violence between humans or animals with machine-on-machine conflict, shifting aggression into a controlled technological domain.

[24] 'Carne coltivata', Wikipedia <https://it.wikipedia.org/wiki/Carne_coltivata> accessed 15 July 2025; L Battaglia, 'Verso nuovi stili di vita. L'avvento della carne a base cellulare' (currently being published).

[25] See P Benanti, *L'hamburger di Frankenstein. La rivoluzione della carne sintetica* (EDB 2017).

are put forward, but behind weak and unfounded ethical arguments lie the powerful economic interests of farmers and the food industry, which is based on the extermination and suffering of animals, which is truly unjustified today.

Numerous studies have proven the nutritional value, taste and production potential of cultivated meat with a significantly reduced impact on animal life. Nevertheless, there is a lack of political will to make truly sustainable choices, as demonstrated by the European governance's actions to date, including recent ones, in the field of cereal farming and intensive livestock farming, which have contributed to financing these practices and limited themselves to measures relating to emissions.

Moving on to alternative techniques to in vivo experimentation, here too technological progress is ready to offer valid solutions with the development in the laboratory of organoids from human and/or animal stem cells.[26] Similarly, 3D printing of organs is a viable option that should be implemented for various experimental purposes.[27]

In any case, even if further efforts are needed to achieve reassuring results, organoids are certainly a useful tool for avoiding xenotransplantation, *i.e.* the transplantation of organs taken from hybrid animals bred in laboratories solely as incubators for organs intended for humans. Xenotransplantation opens up another chapter in the serial and industrial exploitation of animals.

Here too, funding could go in one direction – that of sustainability in the name of protecting vulnerability – but instead it goes in another. The scientific community is calling for a further postponement of the entry into force in Italy of Legislative Decree No. 26/2014, implementing EU Directive No. 2010/63/EU on the protection of animals used for scientific purposes. The decree is at the centre of a strong controversy in the scientific community because it introduces (in Article 5, paragraphs 2d and 2e) stricter prohibitions than those provided for in the Directive itself regarding the use of animals for experiments on xenotransplantation and for research on substances of abuse. In 2016, the EU Commission itself initiated infringement proceedings against Italy for incorrect transposition of the Directive: these proceedings are still ongoing and have not been referred to the Court of Justice.

The current government had further postponed the entry into force of Article 5 of the Legislative Decree until 2025, while the ban on the breeding of dogs, cats and non-human primates for experimental purposes (Article 10, Legislative Decree No. 26/2014) continues to be in force in our legal system. This ban is also ineffective as it is not accompanied by a ban on the use of non-breedable animals, which are therefore imported from abroad and used for experimental purposes!

---

[26] S Landini and others, 'Ethical-legal aspects of organoids and their use in research. Manage risks and legal constraints for the development of ethical research' (2023) EJPLT 34-44; M Cassotta and others, 'Modernizing gut-brain axis research in nutritional science: The role of human-centered New Approach Methodologies' (2025) 159(4) Trends in Food Science & Technology 137, 133–142. Recently the really important lecture of Prof. Anna Maria Bassi 'Il progresso nella tecnologia e le alternative etiche e scientificamente superiori ai metodi tradizionali di sperimentazione animale' (Seminars Cycle of Italian Institut of Bioetics: <https://www.istitutobioetica.it/>), has clearly lightened the role of organoids in the medical research.

[27] G Schinaia, 'Stampa 3D di organi umani, nasce in Italia il primo laboratorio' Wired (29 July 2024) <https://www.wired.it/article/stampa-3d-organi-umani-medicina-universita-statale-milano/>.

On 2 December 2025, Legislative Decree no. no. 183 which amended Legislative Decree no. 26 of 4 March 2014, implementing Directive (EU) 2024/1262, amending Directive 2010/63/EU as regards requirements for establishments and for the care and housing of animals and as regards methods of killing animals. (25G00191). The measure entered into force on 19/12/2025 but does not reduce the number of animals that can be used; it does not prohibit particularly sensitive species (primates, dogs, cats); updates suppression methods, but does not delete them; It focuses on structural requirements, not a mandatory transition to alternative methods.

Adding to this contradictory picture are the latest news reports[28] on xenotransplantation, which continues to be rejected or, in any case, does not integrate with the human host body, as was already reported years ago by the most active animal rights associations[29] and continues to be highlighted today, especially by the medical research community, which is attentive to these issues and genuinely intent on finding alternatives.[30]

It should be noted that divisions have also emerged on this issue within the National Bioethics Committee (CNB), which in March 2020, with 26 members in favour and 6 against, approved a motion to revoke the prohibitions laid down in the implementing decree of Directive 2010/63. However, the six votes against raised strong ethical objections to xenotransplantation. In particular, Luisa Battaglia of the University of Genoa, bioethicist and President of the Italian Institute of Bioethics, stated that xenotransplantation is a 'serious' case of animal exploitation and that the shortage of donors should be resolved by increasing human donations.

It should also be remembered that Article 13 of Law No. 40/2004, entitled «Experimentation on human embryos», is in force in our legal system, which categorically prohibits, without distinction as to purpose, «the fertilisation of a human gamete with a gamete of a different species and the production of hybrids or chimeras»; the wording of the provision is very broad and essentially establishes a general prohibition on the production of hybrids or chimeras, regardless of other operations. Regardless, therefore, of the implementation of Directive 2010/63, the ban on the production of hybrids or chimeras for any purpose (in which no obstacles to the inclusion of xenotransplantation appear to be found in terms of technical interpretation) has been in force in our legal system for some time, and a careful interpretation of the same would place it ahead in the process of repositioning human beings in their relationship with other living beings, at least on this level.

In this area of in vitro experimentation as an alternative to in vivo experimentation, there is also a clear lack of political will at various levels to make real sustainable choices. Thus, the logic of human domination over all

[28] E Mullin, 'Perché un rene di maiale ogm trapiantato in una donna è durato due mesi' Wired (9 June 2024) https://www.wired.it/article/trapianto-rene-maiale-rimozione-lisa-pisano/.

[29] M Kuan, 'Embrione pecora-uomo, ricerche fallimentari alimentano business e false speranze' LAV (19 February 2018) <https://www.lav.it/news/embrione-pecora-uomo>.

[30] L Battaglia, *Un'etica per il mondo vivente: Questioni di bioetica medica, ambientale, animale* (Carocci 2011); C Rovida, 'Sviluppo e applicazione di metodi in vitro e in silico avanzati nella UE' (December 2023) EJPLT Observatory <https://www.ejplt.tatodpr.eu>; IR Pavone, 'L'attuazione della Direttiva 2010/63/UE in Italia: profili critici' (December 2023) EJPLT Observatory <https://www.ejplt.tatodpr.eu>.

other living beings and over the weakest members of their own species continues to be perpetuated.

7. Conclusions.

In 2022, it was written in our Constitution that the Italian Republic must safeguard, protect, preserve and, therefore, not kill or destroy animals, the environment and ecosystems. But how much are these words worth if, instead, the rights not to be eaten industrially and not to be subjected to medical experimentation are not effectively recognised for non-human living beings?

There is still a long way to go because the relational idea of vulnerability, which sees the subject of law as a guardian and no longer as a dominator, is a long and complex path, and at this moment we are not even halfway there because it is easier to avoid facing the complexity of our role.[31]

Today, some of the humans living on the planet kill animals for pleasure, eat them industrially, exploit plants without limits (even genetically modifying them), experiment on animals causing them suffering and death, and ghettoise indigenous peoples, depriving them of their natural habitats.

Human rights are extolled on paper, but we are enveloped in a drive to reify living beings, involving human beings themselves in their most fragile and vulnerable forms, such as economically weaker peoples, culturally diverse peoples, but also embryos and genetic heritage (not to mention the numerous wars currently underway, which represent a real setback in the evolutionary process of human beings as guardians of vulnerable living beings).

Our journey towards protecting other living beings, both animal and vegetable (and human), is effectively only just beginning. We are only now becoming aware that not everything is permitted simply because human beings (in some parts of the planet) have, for various reasons, attributed to themselves legal subjectivity, understood as the power of life and death over other living beings around them.

The hope is that the new generations will take up these demands for sustainability, understood as the protection of the vulnerability of non-human living beings (but also of the weakest humans), and carry them forward with courage, directing technological development towards the genuine well-being of the planet first, and then of humanity.

[31] L Battaglia, *Uomo, natura, animali: Per una bioetica della complessità* (Altravista 2016).

Gatt L, Lo Conte MT, Mazzarella ME, 'Analysis and perspectives on the AI Act: scope and impact assessment' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252LGMTLCMEM

EJPLT
ISSN 2704-8012



Analysis and perspectives on the AI Act: scope and impact assessment

Analisi e prospettive dell'AI Act: ambito di applicazione e valutazione d'impatto

LUCILLA GATT
Full Professor of Private Law, Suor Orsola Benincasa University of Naples
Director, Research Centre of European Private Law (ReCEPL)

MARIA TERESA LO CONTE
Junior Researcher, Research Centre of European Private Law (ReCEPL)
Ph.D. student, Università degli Studi di Roma "Tor Vergata"

MARIA EUGENIA MAZZARELLA
Ph.D. student, Scuola Superiore Meridionale

Abstract

The article specifically examines the AI Act by analysing its objective, subjective and territorial scope. After an examination of the actors involved, dwelling on all the actors mentioned in the Regulation, the risk-based approach of AI systems and models is analysed, and the specific obligations of the actors along the AI chain of responsibility are outlined. Particular emphasis is then placed on the Fundamental Rights Impact Assessment (FRIA) and the ethical and legal challenges posed by generative AI, emphasising the need for an anthropocentric approach and governance that safeguards human rights in the digital age. Finally, the contribution also reflects on the role of AI in democratic life and its influence on information and political power.

* This article is the updated version, translated in English of the contribution L Gatt, MT Lo Conte, ME Mazzarella, 'L'ambito di applicazione, soggettivo e oggettivo, dell'AI Act' in U. Ruffolo (ed.), *AI Act - La regolamentazione europea dell'Intelligenza artificiale* (Luiss University Press, 2025), 49 ff.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
L'articolo esamina in modo specifico il Regolamento dell'Unione Europea sull'Intelligenza Artificiale (AI Act) analizzandone l'ambito di applicazione oggettivo, soggettivo e territoriale. Dopo la disamina dei soggetti coinvolti, soffermandosi su tutti gli attori menzionati dal Regolamento, viene analizzato l'approccio basato sul richio dei sistemi e modelli di IA enucleando inoltre gli specifici obblighi degli attori lungo la catena di responsabilità dell'IA. Particolare enfasi viene poi posta sulla valutazione d'impatto dei diritti fondamentali (Fundamental Rights Impact Assessment - FRIA) e sulle sfide etiche e legali poste dall'IA generativa, sottolineando la necessità di un approccio antropocentrico e di una governance che salvaguardi i diritti umani nell'era digitale. Il contributo riflette in ultimo anche sul ruolo dell'IA nella vita democratica e sulla sua influenza sull'informazione e sul potere politico.

Keywords: AI Act; Application; AI Systems; AI Models; FRIA

Summary: 1. Introduction. – 2. Territorial and material scope. – 3. Subjective scope. – 3.1 Provider. – 3.1.1 Extra-Providers. – 3.1.1.a Prospective provider. – 3.1.1.b Downstream provider. – 3.2 Product Manufacturer. – 3.3 Deployer. – 3.4 Other Operators. – 3.5 Interposing Subjects. – 3.6 Institutional Actors. – 4. Objective Scope. – 4.1 AI Systems. – 4.1.1 Prohibited AI practices. – 4.1.2 High-risk AI systems. – 4.2 General Purpose AI Models. – 4.2.1 Systemic AI Models. – 4.2.2 Generic AI Models. – 4.2.3 Certain AI systems. – 5. FRIA - Fundamental Rights Impact Assessment – 5.1 Possible new developments. – 6. Conclusions.

1. Introduction.

In the long process of European Union standardisation, the subject of Artificial Intelligence has gone through a tortuous path of proposals, opinions and corrigenda, but 21 May 2024 saw the final decision by the Council of the European Union:[1] the Artificial Intelligence Act (now and henceforth 'AI Act') is law (*rectius* Regulation) and in its final version aims to regulate the use of Artificial Intelligence (now and henceforth 'AI') in the territory of the Union.

The AI that is the subject of EU regulation is understood in a broad and dynamic sense in order to remain relevant in the rapid course of technological innovation. Pursuant to Article 3(1)(1), in going on to specify Recitals 12 and 4, the 'AI system' that is the subject of this regulation is in fact defined as an automated system that, jointly:

- is designed to operate with varying levels of autonomy;
- can be adaptable after deployment;
- deduces from the input it receives how to generate output (in the guise of predictions, content, recommendations and decisions) that can influence both physical and virtual environments.

[1] Council of the EU (2024, 21 may) Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/
Vote: eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CONSIL:ST_10199_2024_INIT

Having established a clear, comprehensive, and inclusive definition of AI and identified its fundamental characteristics – autonomy, adaptability, and generativity – it is widely recognized that AI refers to technologies designed to replicate human intellect and cognitive abilities, such as learning and problem-solving, with the goal of performing tasks in real-world contexts.[2]

To establish a uniform legal framework for the development, market placement, deployment, and use of safe, reliable, ethical, and human-centered AI systems, the EU legislator immediately recognized the necessity of harmonized protection across Member States, balancing the risks and benefits of AI. Indeed, given the exponential use of AI, it naturally brings economic, environmental, and social benefits, yet it also inevitably presents inherent risks. These include potential infringements on public interests and fundamental rights, as well as possible 'physical, psychological, social, or economic harm'.

To understand this ambivalence of new technologies, we must take a brief step back.

In the field of AI, a longstanding debate exists between proponents of engineering-reproductive AI and semantic-productive AI. The former is characterized by AI systems that replicate, in the sense of copying, certain human behaviors through algorithms programmed by engineers and developers. The latter focuses on developing machines and digital systems capable of functioning entirely autonomously, learning from their experience (essentially their operational processes, i.e., machine learning), and potentially surpassing human capabilities. So far, the first category has produced the most concrete and operationally manageable results, though research into the second type is advancing rapidly. This fuels collective imagination, as these AI systems can manage complex situations and make autonomous, unforeseen, and unpredictable decisions – this so-called 'strong AI' is, unsurprisingly, the most challenging in terms of human control and regulatory oversight.

Since the Dartmouth College conference in 1956, where the term 'Artificial Intelligence' was first coined for a branch of computational informatics that had already been in development for some time, the field has experienced alternating periods of significant and modest investment (the so-called AI 'springs and winters').

In the last decade, investments in new technologies have surged dramatically, mainly due to two factors: a significant increase in computational power and the vast amount of data available to train AI algorithms, coupled with a reduction in sensor costs, which facilitate data collection.

Generative AI, in particular, has undergone exceptional development: it has demonstrated an unprecedented ability to generate digital content surpassing anything previously created by humans. However, although GenAI can produce new content, but cannot currently generate new ideas or solutions to real-world challenges, as it does not understand the social connections or relationships underlying the language or content provided to it. [3] These systems still lack autonomous semantic capability. Generative AI systems based on large language models (LLMs) operate purely on statistical reasoning and

[2] IBM, 'Cos'è l'intelligenza artificiale (AI)?' (*IBM*) <www.ibm.com/it-it/topics/artificial-intelligence>.

[3] S da Empoli, R Loiero, 'L'Intelligenza Artificiale tra rischi e opportunità' in R. Razzante (ed.), *Manuale sull'Intelligenza Artificiale* (Giappichelli Editore 2024) 33.

probability. This functional model has led some authors to describe AI as *agere sine intelligere* (acting without understanding).[4]

Artificial Intelligence, in general, can be considered a dual-faced concept. Just as a knife can be both a useful tool for nourishment and a weapon for harm, so-called intelligent technologies offer significant opportunities as well as risks. AI systems can replace humans in dangerous, exhausting, and repetitive tasks (e.g., applications in agriculture, industry, and military sectors). They can also predict human behavior, identify diseases early, and assess risks to people's interests and well-being.

Thus, if today we can discuss soft robotics[5] in healthcare and robotic surgery, if the latest robotic innovations are presented annually at the World FIRA in agriculture, and if, along with logistics, these fields have been identified by the International Federation of Robotics in World Robotics 2023[6] as three of the five key areas for the deployment of so-called Professional Service Robots, it is undoubtedly thanks to both the *homo faber* who has transformed into the *homo creator* – a producer of artificial nature – [7] and the continuous advancements in AI and its associated benefits.

Beyond these advantages, however, generative AI systems can have ambivalent effects on productivity, economic growth, and especially employment. Other risks concern potential violations of individual privacy and fundamental rights in general, with the possibility of perpetuating large-scale discriminatory patterns.

This broad range of opportunities and risks stems from the intrinsic characteristics of generative AI, which many experts classify as a so-called general-purpose technology (GPT) due to its pervasiveness (it can be applied across multiple sectors), its high potential for technological development, and its complementarity with other technological innovations.[8]

Although previous predictions of widespread mechanization of the production sector have not materialized, generative AI could still enhance productivity in several ways. Firstly, its ability to replace humans in certain tasks – whether manual or intellectual – allows individuals to focus on more productive activities. Moreover, those forced to change jobs may find new opportunities, potentially created by future AI implementations. This could provide greater opportunities for younger generations, who are more inclined to develop digital skills, but at the same time, it might disadvantage those in advanced career stages who may struggle to acquire new competencies (digital divide).

The public and academic debate of the past decade regarding AI's effects on employment has been divided between a positive perspective – arguing that AI systems would boost productivity, significantly optimize economic processes, and negatively impact only a limited number of job roles – and a negative view,

---

[4] L Floridi, F Cabitza, *Intelligenza Artificiale. L'uso delle nuove macchine* (Bompiani 2021).

[5] M Yip and others 'Artificial intelligence meets medical robotics' (2023) 381(6654) Science 141 – 146.

[6] See International Federation of Robotics, *World Robotics* (2023) 36. <https://ifr.org/img/worldrobotics/2023_WR_extended_version.pdf>

[7] PP Portinaro, 'Introduzione' in PP Portinaro (ed.), *Il principio di responsabilità. Un'etica per la civiltà tecnologica* (Einaudi 2009) XXIV.

[8] TH Bresnahan, M Trajtenberg, 'General purpose technologies 'Engines of growth'?' (1995) 65(1) Journal of Econometrics 83-108.

predicting a near-total replacement of human workers in both manual and intellectual tasks, leading to widespread unemployment.

As is often the case, the truth lies somewhere in the middle. Recently, two studies – conducted by the OECD (2023) and the International Monetary Fund (2024) – have analyzed AI's potential impact on the labor market.

The OECD report focused on AI in general, highlighting that AI will replace certain human jobs (displacement effect), but it can also increase labor demand due to productivity growth (productivity effect) and AI may also create new job opportunities (reintegration effect).[9] The most at-risk workers are those with low qualifications: according to the OECD, occupations at risk of automation account for 27% of total employment, rising to 30% in Italy.

The International Monetary Fund study focused on generative AI's impact on employment by applying an index measuring the exposure and complementarity of human labor concerning AI. According to this index, high exposure reduces labor demand, while high complementarity can increase it by boosting productivity through human-machine collaboration, provided workers possess adequate skills.[10] The IMF estimates that 40% of jobs are at risk of automation, increasing to 60% in advanced economies.

Other negative impacts on fundamental rights such as privacy are due to the structural flaws of new technologies: new generative AI chat-bots can produce so-called hallucinations, i.e. false but truthful content. These incorrect out-puts can influence public opinion and through the improper treatment of personal data damage the privacy and potentially the dignity and reputation of those involved, as was the case with Brian Hood, now mayor of an Australian city, who had denounced the wrongdoings of the company he worked for, but whom Chat-GPT identified as one of those actively involved in the scandal.

The exceptional potential accompanied by equal risks of the new technologies must push those in charge of their governance to lay the foundations for a sustainable digital transition by setting up a clear regulatory framework, of which the regulation that is the subject of this contribution is a commendable starting point.

With regard to the purpose and subject matter of the AI Act, the legislator, in Article 1, specifying Recitals 1-6 and 8 and briefly anticipating the content of the legislation, states that the Regulation introduces a real set of harmonised rules for the use and market of artificial intelligence systems in the EU, providing both prohibitions for certain types of practices and specific requirements for certain systems and models, but at the same time also providing for monitoring, supervision and support measures for innovation, with particular attention to SMEs and start-ups.

2. Territorial and material scope.

In defining this scope of application, it is essential to clarify from the outset that the actors of the AI Act must comply with the obligations of the Regulation in a non-discriminatory manner, regardless of their place of establishment,

[9] da Empoli, Loiero (n 2) 42.
[10] da Empoli, Loiero (n 2) 42.

location, or physical presence. In this regard, the Regulation has intentionally introduced the so-called Brussels effect to indirectly extend its provisions beyond the geographical boundaries of the European Union. This intent is further reinforced in Article 2 of the Regulation, which explicitly states that it applies to providers [and deployers] established or located in a third country outside the EU if the outputs of the AI system are used within the Union, as well as to Authorised Representatives of providers not established in the Union.

In light of this strategy, the European legislator – drawing from the experience of the GDPR and the EDPB Guidelines[11] – has chosen to combine the principle of establishment with an approach that more effectively considers the influence (and legal authority) of the European Union. This applies whether the providers are located within the Union or in a third country, whether the deployers are situated within the Union, or whether providers or deployers of AI systems from non-EU countries intend to use them within the EU. On this point, under the AI Act, territorial considerations become irrelevant due to the introduction of a Union-centric approach, taking into account the fact that the world's leading AI powers are not European.

In this regard, the European legislator has defined a precise characteristic of this regulation: whenever an AI system is placed on the market or put into service in Europe, or whenever the output of an AI system has an impact on the territory, market, or individuals within the Union, it must necessarily be subject to this Regulation in order to safeguard the internal market and the fundamental rights and freedoms of EU citizens.

However, it is important to note that this extension – sectorally speaking – is not unlimited: the Regulation applies only to sectors falling within the scope of EU law. In this sense, it has struck the right balance in strengthening the European Single Market while simultaneously ensuring the outright exclusion of the potentially harmful impacts of a – albeit utopian – Korean-style Data Dam[12], which envisions total data openness for AI training. By asserting the supremacy of EU law in the face of AI economic giants, the Regulation has imposed its unequivocal compliance as a condicio sine qua non for any international entity seeking to operate in the AI market within the Union.

3. Subjective scope.

While a first reading of the Regulation may suggest that its scope of application is outlined in the aforementioned Article 2, a thorough examination of the entire text is essential to understand that the actors involved are numerous and diverse. The entities concerned can be categorized into two main groups – Operators and Institutional Actors – which, despite comprising distinct and well-defined subjects, maintain multiple points of interaction and

[11] European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)' (2018) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf>.

[12] Republic of Korea Ministry of Science and ICT (2020, 2 Sept), Data Dam project begins, being key to Digital New Deal [Press Release] <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=453>.

reciprocal implications. The Provider, the product manufacturer, the deployer, the Authorised Representative, the importer, and the distributor all belong to the category of Operators, as each operates within the AI value chain, and the Regulation assigns each of them specific obligations, rights, duties, and prerogatives. At the same time, Institutional Actors are manifold, some newly introduced, others long established: the AI Office, the Market Surveillance Authority, the Enforcement Authority, and the European Commission are some examples. Finally, there are additional entities that, acting as Intermediary Subjects, are either involved in the activities of Operators or necessary for the practical implementation of the AI Act (Fig. 1). Moreover, while the notion of Operator is explicitly provided by Article 3, paragraph 1, point 7 of the AI Act, and other entities are regulated either explicitly or implicitly, it becomes evident that a true understanding of the AI Act often requires looking beyond the formal qualification assigned to them by the Regulation.

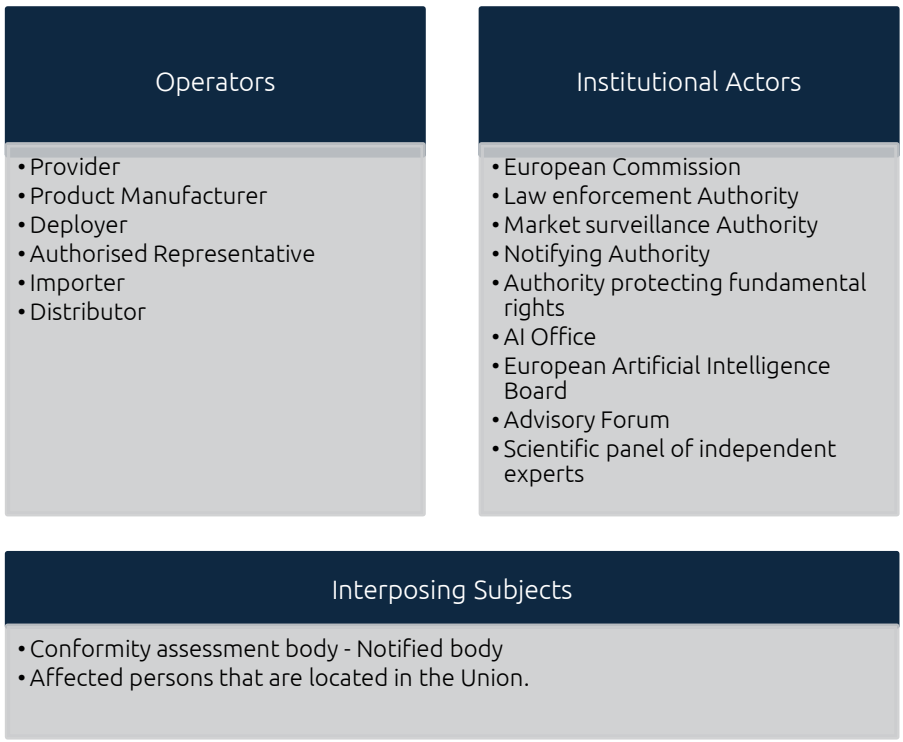


Fig. 1

3.1 Provider.

Among the Operators, the first entities to be highlighted are Providers, namely all those – whether natural persons, legal entities, public authorities, agencies, or other organizations – that develop or have third parties develop an AI system or a general-purpose AI model and subsequently, separately:

- place the AI system or general-purpose AI model on the market, meaning its initial availability on the Union market;

- put the AI system into service under their own name or brand, for any purpose (whether for consideration or free of charge), meaning the provision of such a system by the Provider to the deployer for first use or for their own use in the Union market.

The definition of Provider, as established in Article 3, paragraph 1, point 3 of the AI Act, appears to be all-encompassing, as it does not make formal distinctions between public, private, institutional, or non-institutional entities but instead assesses their actual activities and thus their substantive qualification. This entity is responsible for the placement on the market or the putting into service of an AI system, particularly if it is high-risk. Furthermore, while AI literacy remains necessary to equip Providers with the knowledge required to make informed decisions about AI systems, they are subject to various highly detailed obligations, depending on the specific AI system or model involved.

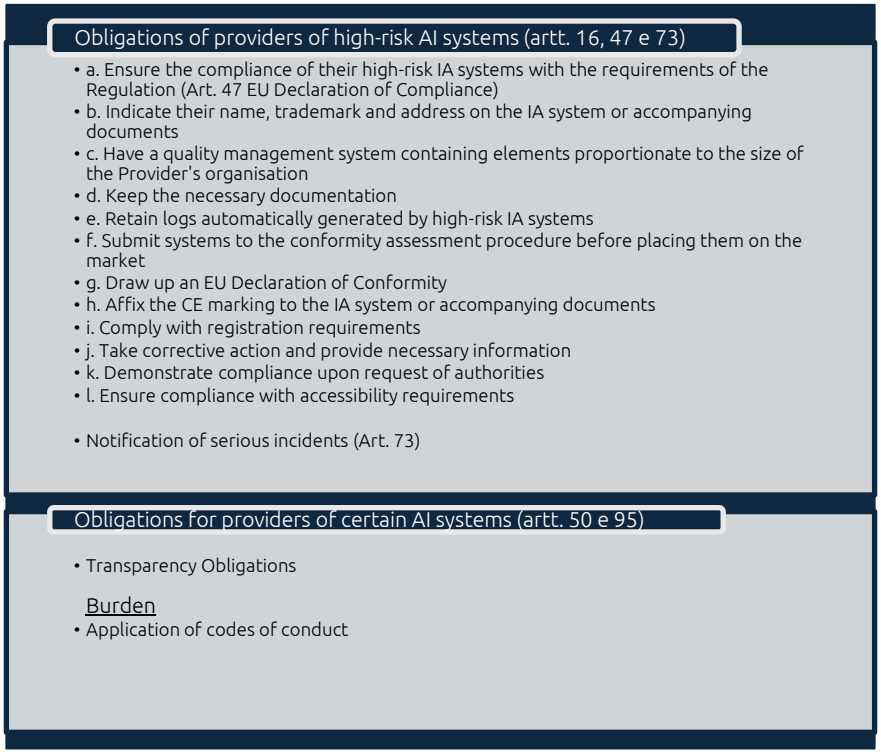


Fig. 2

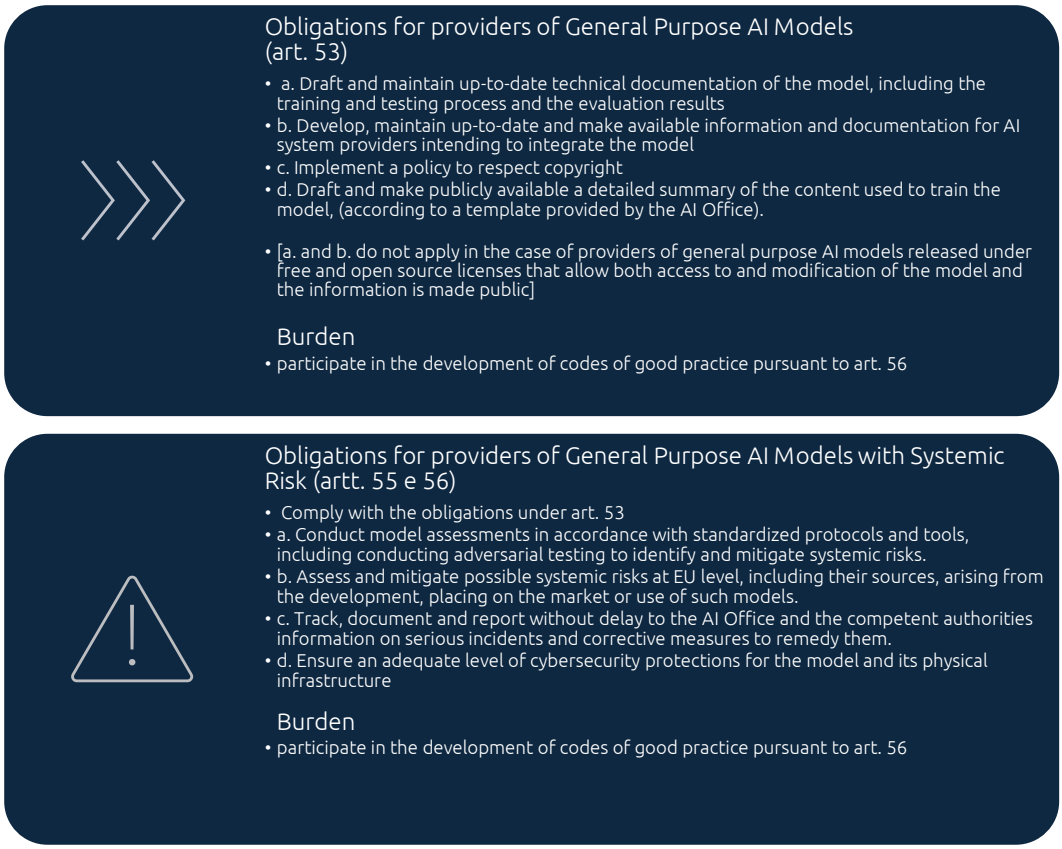


Fig. 3

3.1.1 Extra-Providers.

Alongside the figure of the so-called pure provider, it appears necessary to identify further figures: that of the prospective provider and the downstream provider.

3.1.1.a Prospective provider.

With regard to the Prospective provider, the AI Act does not provide a specific definition. Therefore, it is undoubtedly necessary to refer to the general definition set out in Article 3 of the AI Act, but understanding it in the merely potential form of its typical activities: development and putting into service or placing on the market.

This definition appears necessary, as it is not possible to include this figure among the 'affected persons' under Article 2, paragraph 1, letter g) of the Regulation; this concept only includes individuals who 'are located in the Union', whereas a prospective provider could very well be located outside EU territory and engage in practices that circumvent the Regulation.

This extension of meaning can be traced to the rationale of the AI Act and the Union legislator's intention to encompass as broad a subjective scope as possible, provided that the AI output affects the European market. Confirmation of this interpretation can primarily be found in Recitals 140 and

141, but above all within the main text, where prospective providers are explicitly included among the entities authorized to develop, train, validate, and test an innovative AI system in a regulatory sandbox.

At the same time, a specific procedure is established: they must agree on a detailed experimentation plan with the competent authority and be monitored by the authorities to ensure compliance – both regulatory and procedural – with the AI Act.

3.1.1.b The Downstream provider.

The Downstream provider perfectly fits into the so-called AI supply chain, representing the first key entity in the most complex scenario of an AI system integrating an AI model. As highlighted in Article 3, paragraph 1, number 68) of the AI Act, it is essential to specify that such a model can either be supplied directly by the same downstream Provider (and then vertically integrated by them) or provided by another external entity based on contractual agreements, followed by the subsequent integration of the model into an AI system by the downstream Provider. In the second scenario, specific complexities arise when an AI system is integrated with a general-purpose AI model, as general-purpose AI models – supplied by their respective providers – often form the foundation of downstream systems provided by downstream providers. (Fig. 4)

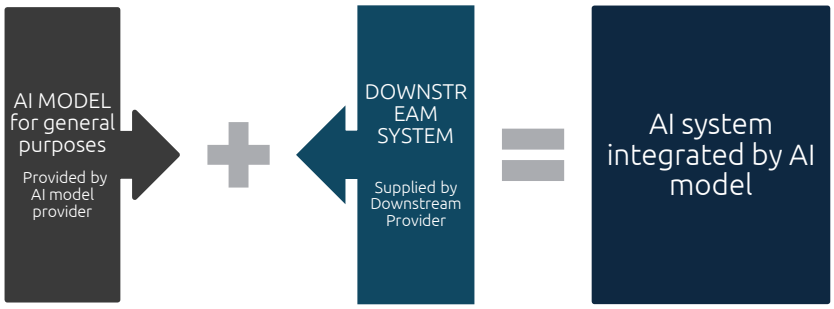


Fig. 4

In light of this significant connection between the two entities – both 'providers' but with different qualifications – the Regulation establishes specific transparency measures for the former when supplying general-purpose AI models. These measures ensure that the downstream Provider wishing to use a given AI model for its system is aware of its characteristics and can, in turn, comply with the obligations set out in the Regulation.

To foster a proper understanding of general-purpose models and their actual capabilities, the Regulation, in Recital 101, considers it appropriate to impose proportionate transparency measures on the model Provider. These include drafting and updating documentation and the general 'provision of information' on the general-purpose AI model to facilitate its use by downstream providers, incorporating all the indications listed in Annex XII of the AI Act.

At the same time, regarding obligations, reference is undoubtedly made to the requirement to label non-human outputs created by AI, the so-called

synthetic content. Recital 133 explicitly supports this, facilitating compliance for the downstream Provider of the AI system. If this operation is performed upstream by the Provider of the general-purpose AI model, it undoubtedly simplifies the work of the downstream Provider, who, in this case, supplies a general-purpose AI system integrating a general-purpose AI model.

It is evident that the EU legislator assigns particular importance to the figure of the downstream Provider. This is confirmed from Recital 162, which anticipates Article 89 of the AI Act and foresees its involvement in effective monitoring activities carried out by the AI Office. In fact, within the monitoring actions for enforcing obligations imposed on providers of general-purpose AI models, entrusted to the AI Office by the European Commission, the downstream Provider serves as the trait d'union between economic and institutional actors. It is formally granted, under Article 89(2) of the AI Act, the right to file complaints regarding potential violations of the Regulation by providers of AI models and general-purpose AI systems.

Due to its monitoring responsibilities, the downstream Provider benefits from the protections that the Regulation grants to so-called informants or whistleblowers, particularly those outlined in Directive (EU) 2019/1937[13], as stipulated in Recital 172 of the Regulation.

Finally, in light of the strong emphasis placed on soft law measures, especially codes of good practice, the downstream Provider is explicitly included in Article 56(3) among those entities eligible to support the development of such measures.

In conclusion, it is possible to affirm that the downstream Provider, beyond acting as a warning signal regarding the conduct of the entities from which it sources materials or models for its system, also plays a primary role in regulating them.

3.2 Product Manufacturer.

The figure of the Product Manufacturer represents another Operator under the AI Act when it proceeds to place on the market (i.e., the first making available in the Union Market) or put into service (i.e., direct supply to the deployer for first use or own use in the Union for the intended purpose) an AI system together with its product. This makes it a figure very close to that of the Provider.

It is worth noting that this figure is understood as the one who manufactures a product in which the safety component is represented by an AI system, although it is generally referred to as a commercial entity responsible for the production of final products – falling within the scope of Union harmonization legislation – that incorporate a high-risk AI system as a safety component. Considering that such high-risk systems used as safety components could negatively impact people's health and safety, even while aiming to facilitate the free movement of products in the internal market, there remained the need to prevent and mitigate the safety risks of such products. In light of these needs, on the one hand, the Regulation has classified all AI systems that serve

[13] Parliament and Council Directive 2019/1937/EU of 23 October 2019 on the protection of persons who report breaches of Union law [2019] OJ L305/17. <https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng>

as safety components of products (or that are products themselves) as 'high-risk systems' when the affected product (such as machinery, toys, pressure equipment, or medical devices) is subject to a conformity assessment by a third-party conformity assessment body, as provided in Recital 50. On the other hand, Recital 51 states that products based on the same system classified as 'high-risk' are not necessarily required to be classified as 'high-risk' under the harmonization legislation applicable to products. At the same time, AI systems linked to non-high-risk products, while not required to comply with the requirements set for a high-risk AI system, must still be safe when placed on the market or put into service.

The Regulation further stipulates that a manufacturer may assume the role of Provider and thus be subject to the corresponding obligations imposed on the latter, as a result of the responsibility along the AI value chain anticipated in Recital 87 and detailed in Article 25(3) of the AI Act. This occurs when, in the case of high-risk AI systems serving as safety components of a product, the AI system is placed on the market together with the product under the manufacturer's name or trademark, or when the product is initially put into service, followed later by the AI system under the same manufacturer's name or trademark.

3.3 Deployer.

The deployer represents a newly defined figure, described as the 'natural or legal person, public authority, agency or other body using an AI system under its authority', according to Article 3, paragraph 1, point 4, AI Act. For this subject, the centrality of professional activity is of particular relevance, as the Regulation explicitly excludes from this subjective category those who use the AI system «in the course of a non-professional personal activity».

Once again, the need to provide AI literacy remains essential to equip the deployer with the necessary knowledge to make informed decisions regarding AI systems. Various obligations are placed on the deployer, especially in the case of high-risk systems, as outlined in Article 26. (Fig. 5)

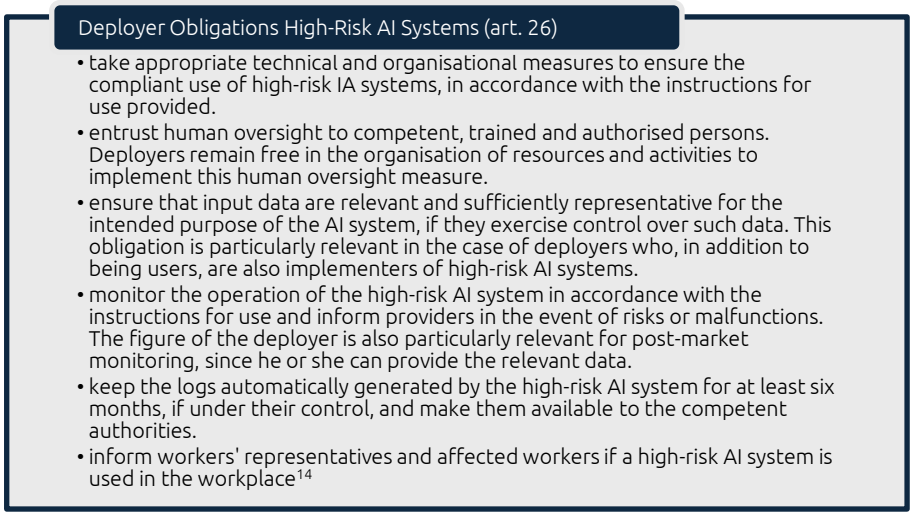


Fig. 5

Additionally, for certain subjects, further obligations are added, including the requirement for an impact assessment on fundamental rights of high-risk AI systems. This activity, as will be discussed later, is limited to the subjects indicated in paragraph 1 of Article 27 AI Act, and these subjects, at the time of the first use of a high-risk AI system, are required to describe the process and frequency of use, the categories of individuals involved, and a specific description of the risks to which these individuals will be exposed, with particular attention to monitoring measures and those aimed at mitigating them. It is clear that in this case, the European legislator, not being in a position to know the specific risks associated with a given AI system, leaves the individual deployer with the responsibility to assess them through a self-assessment of their own safety framework and requires communication of the results to the market surveillance authority.

Moreover, still within the scope of high-risk systems, in the case of deployers of emotion recognition systems or biometric categorization systems, they are required to inform individuals exposed to the functioning of the system, unless these systems have been authorized by law for the purpose of investigating, preventing, or detecting crimes.

On the other hand, in the context of generative AI, with the creation of so-called deepfakes [15] and systems that generate or manipulate texts for information purposes, the deployer is required to disclose that the text was created or modified by AI. All these information obligations placed on the deployer also have a precise temporal requirement – 'at the latest at the time of the first interaction or exposure' – and must be accessible.[16] It is clear that these provisions were designed to protect individuals exposed to synthetic content and to make it clear to them that they are interacting with a machine, not a human being.

In conclusion, it should be emphasized that in this case, the mechanism protecting the market introduced by the European legislator is of particular importance: the system of liability along the AI value chain. If certain subjects, including deployers – but also importers, distributors, or other third parties – engage in particularly impactful actions on the system, such as making substantial changes to the system or modifying the purpose of a non-high-risk system, precise consequences are triggered: in such cases, the initial Provider will no longer be considered as such for that system (although their obligation to cooperate for information or support remains), and the deployer (or anyone else acting on their behalf) must also comply with the obligations placed on the Supplier. Through this solution, the AI Act has established a key principle:

[14] For an initial assessment of the organizational impacts of the new regulations concerning the obligations for the user (deployer) of high-risk AI systems when used by an employer, see L Barbieri, A Rossetti 'Sistemi d'intelligenza artificiale ad alto rischio e obblighi del datore di lavoro' 2024 Norme&TributiPlus. The authors, in illustrating in practical terms the provisions of both Article 26 and Recital 92 of the AI Act, not only analyze the obligations imposed on the 4.0 employer, but also focus on the principle of transparency and information in favor of the worker, as well as the need for human oversight and a dedicated management system to 'counter, prevent, or minimize risks to health, safety, or fundamental rights that may arise'.

[15] These are images, audio, or videos generated or manipulated by AI to resemble real persons, objects, places, events, or entities, which may appear deceptively authentic or true.

[16] Art. 50, par. 5, AI Act.

whenever a system is modified, the entity making the modification is required to ensure its compliance.

3.4 Other Operators.

Alongside the aforementioned subjects, additional figures emerge: these are figures that are, in some cases, optional, but in others, essential in the so-called AI supply chain. The Authorised Representative and the Importer are operators provided for by the regulation only when the Provider of a high-risk AI system or a general-purpose AI model is a non-EU Provider, established in a third country.

In order to ensure that, under any circumstances, a person established in the Union can provide the authorities with all the necessary information on the compliance of an AI system, the AI Act has established the figure of the Authorised Representative. The Supplier of high-risk AI systems established in a third country must appoint this Representative through a written mandate before making the system available. The Representative will then be authorized to perform the tasks specified in the Supplier's mandate and indicated in Article 22 of the Regulation for high-risk AI systems. Similarly, this obligation is placed on suppliers of general-purpose AI models, except for suppliers of general-purpose AI models released under a free and open-source license that do not present systemic risks under Article 54 of the Regulation, although with the provision of different specific tasks entrusted to the Representative.

The figure of the Importer becomes relevant when it places a high-risk AI system on the EU market that was purchased from a non-EU Supplier. Given its position, the Importer is tasked with ensuring that the system complies with the Regulation, taking on the obligations set out in Article 23, verifying both the presence of the Authorised Representative appointed by the non-EU Proveder and the technical documentation, as well as the compliance with the conformity assessment procedures and the application of the CE marking. After a positive outcome from these checks, the Importer will proceed to indicate its name or trademark on the packaging or accompanying document of the system, ensuring that its transportation does not compromise its conformity.

The distributor, in turn, represents the intermediary between the Provider or Importer and the third party to whom it will resell the AI system. In an era of segmented production processes, the figure of the distributor is becoming increasingly important, which is why EU lawmakers have foreseen it as the subject that must carry out a series of checks before making a high-risk AI system available on the market – such as ensuring compliance with obligations by the Provider and the Importer – and must manage any non-conformities.

Lastly, it is important to note that, under certain conditions, any Distributor, Importer, Deployer, or other third-party subject could be considered a Provider of a high-risk AI system and, therefore, assume all the related obligations.

3.5 Interposing Subjects.

Among the Interposing Subjects, it is important to highlight primarily the conformity assessment body, which is the entity that, on behalf of third parties, performs conformity assessments, including testing, certification, and inspections. This body is the third party that verifies the conformity of high-risk AI systems to the Regulation before their market placement or deployment, with the aim of ensuring a high level of reliability of the systems. In order to assess the quality management system, the technical documentation, and the related monitoring to issue the corresponding certificates in accordance with Annex VII, the conformity assessment body must assume the role of a notified body. This qualification is granted by the notifying authority of each Member State upon the body's application. The AI Act further identifies sectoral groups for coordinating notified bodies and recognizes the conformity assessment bodies of third countries that must meet the requirements set by the AI Act.

Next, it is necessary to identify the so-called 'affected persons' that are located in the Union under Article 2, paragraph 1, letter g) of the Regulation. In this case, it is undoubtedly implied that this refers to individuals who participate in the real-world testing conditions specified, to whom specific provisions are dedicated under Articles 60 and 61, such as the requirement to obtain their informed consent before participating in the tests, after being 'duly informed' of the objectives of the tests, their duration, rights and guarantees, and many other essential details.

In conclusion, particular attention is paid to SMEs, including startups, in order to continue supporting the innovation process necessary in the field of AI.

3.6 Institutional Actors.

In identifying the subjective scope of application of the AI Act, it is not possible to leave out the Institutional Actors. These, involved in the first instance and in a more active way - since these actors must set up the organisational structures, must carry out the controls, and must ensure even more the performance of their functions - are numerous. Notwithstanding the presence of the European Commission, which approves, investigates, coordinates and modifies, and the Member States, which are called upon to implement, authorise and designate, there are many authorities involved. One refers to the typical law enforcement authorities, market surveillance authorities and authorities protecingt fundamental rights, as well as newly created authorities such as notifying authorities, which have been assigned the task of designating, notifying and monitoring conformity assessment bodies. In addition, there are additional actors:

- AI Office, i.e. that institution that enables the Commission to develop expertise and capacity in the field of AI;
- European Artificial Intelligence Board, i.e. a committee consisting of one representative from each Member State and with the non-voting participation of the EDPB and the AI Office;

- Advisory Forum, to provide technical advice to the Committee and the Commission;
- Scientific panel of independent experts, to support the implementing measures of the Regulation.

4. Objective Scope.

In light of the above, risk has been the evaluation parameter chosen by the legislator, as the need emerged to calibrate precautions and obligations for certain subjects along the AI value chain based on the type of risk that a given category of AI systems might pose. Although it has recently been criticized[17], the risk-based approach has allowed for the establishment of rules tailored to the scope of the risks generated by AI systems, with a broadly precautionary approach in mind. This has translated into a series of mechanisms for the review, supervision, and management of AI systems (continuous monitoring, audits, a multilayered governance system at the European and national levels with authorities and notified bodies, as well as provisions for holding entities providing critical infrastructures accountable) which should provide guarantees against non-compliance applications.

From the framework identified by the legislator, four levels of risk have been identified, depending on the context of use, the potential impacts of the technologies, the application sector and the interested parties. In fact, all other AI applications fall within the zero-risk area not regulated by the AI Act (Fig. 4):

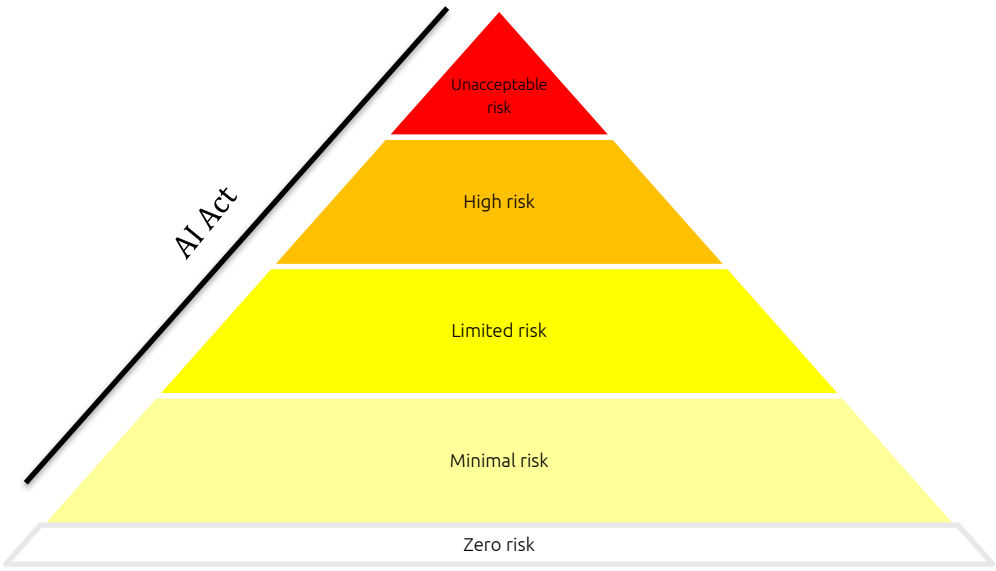


Fig. 4

The Regulation does not govern all AI applications, but only a minority of

[17] F Porzio, 'AI Act, il rischio di danneggiare l'innovazione in Ue' (*Agendadigitale*, 10 May 2024) <https://www.agendadigitale.eu/industry-4-0/ai-act-ecco-come-mette-a-rischio-linnovazione-in-ue-e-con-quali-rischi/>.

them, and from the text emerges a primary distinction between AI systems and AI models. This distinction also allows for overcoming the initial definition of the AI Act as a 'product regulation', as understood at the beginning of the legislative process. In fact, by regulating AI models – those fundamental elements related to the more intrinsic technology that enables the development of an AI system – the Regulation foresightedly governs even the technology underlying the product-system.

Technically, the Regulation, in addition to regulating Artificial Narrow Intelligence (ANI) – the so-called AI systems, or "weak" AI, trained on well-labeled data sets and capable of performing specific tasks in predefined environments – also provides provisions for what will soon be at the core of Artificial General Intelligence (AGI) – the so-called AI systems for general purposes, or "strong" AI, capable of performing a variety of intelligent tasks and adapting to a wide range of situations.

4.1 AI Systems.

With regard to AI systems, the Regulation provides for a differentiated regime of obligations corresponding to the level of risk of the individual system (Fig. 5):

Level of risk	Discipline
Unacceptable risk – Prohibited AI practices	Prohibition regime[except expressly exempted(*ex* art. 5 AI Act)]
High risk – High-risk AI systems	Specific requirements and obligations (*ex* artt. 6 e ss.)
Minimal risk – Certain AI systems	- Transparency Obligations (*ex* art. 50) - Burden of codes of good practice (Art. 56) - Burden of enforcing codes of conduct (*ex* art. 95)

Fig. 5

4.1.1 Prohibited AI practices.

Regarding AI systems with an unacceptable risk, the Regulation establishes a regime of prohibition with the so-called prohibited practices under Article 5 of the AI Act. These include the use of 'subliminal techniques' capable of compromising the ability to make informed decisions, and certain systems that impact individuals' behavior without their awareness, particularly concerning vulnerable groups such as minors, the elderly, and people with physical and mental disabilities. The use of AI systems by public authorities to qualitatively assess individuals is also prohibited, such as the so-called social ranking, which involves assigning scores that lead to measures or actions that impact individuals in an unjustified or disproportionate manner relative to the severity of their behavior. Additionally, the Regulation prohibits AI systems used to assess or predict the likelihood of committing crimes, those that create or expand facial recognition databases through non-targeted scraping of facial images from the internet or CCTV, systems used to recognize the emotions of

individuals in the workplace or educational settings, and those that categorize biometric data to infer race, political beliefs, and similar characteristics.

Furthermore, AI systems used for surveillance of individuals in public spaces via remote real-time biometric identification are prohibited, with a set of exceptions provided for the search of crime victims, missing minors, or for public safety and defense purposes, or for the search of individuals suspected of committing crimes punishable by at least four years of imprisonment. The exceptional use of such systems is subject to a motivated request and prior authorization by the relevant independent authority of the Member State concerned, except in urgent cases where authorization may be sought *ex post*. Each Member State is then responsible for establishing the rules, cases, and limits regarding facial recognition, given its direct impacts on the fundamental rights and freedoms of individuals (under Article 5, paragraph 1, letter d, paragraphs 2 and 4).

It is important to note that non-compliance with the prohibition of the practices outlined in Article 5 is subject to administrative financial penalties under Article 99.

Although the prohibitions set out in this article entered into force on 2 February, the Commission is empowered, pursuant to Article 96, to issue guidance on the practical implementation of the Regulation. To date, the Guidelines on Prohibited AI Practices[18] were published on 4 February 2025, and the Guidelines on the Definition of an AI System[19] under Article 3(1) on 6 February 2025.
The aim of the Guidelines on Prohibited AI Practices is to enhance legal certainty and provide clarity on the Commission's interpretation to ensure the consistent, effective, and uniform application of the prohibitions under Article 5 by competent authorities, providers, and deployers of AI systems.

These guidelines are not binding, and the application of Article 5 will in any case require an assessment based on the specific circumstances of each case. The legal basis of the European Regulation is provided by Articles 114 (internal market) and 16 TFEU (data protection). In particular, Article 114 concerns the adoption of measures relating to the approximation of the legislative, regulatory, and administrative provisions of the Member States that aim at the establishment and functioning of the internal market. Article 16 establishes the right of every person to the protection of personal data concerning them. It refers in particular to the prohibitions on the processing of personal data derived from the use of remote biometric identification systems, the use of biometric categorisation systems, and individual risk assessment for law enforcement purposes. All other prohibitions under Article 5 of the AI Act are

[18] Communication to the Commission "Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (*AI Act*)", Brussels, 4.2.2025 C (2025) 884 final. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.

[19] (Annex to the) Communication to the Commission "Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (*AI Act*)". <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>.

legally based on Article 114.

As set out in the Commission's Guidelines, Article 5 of the AI Act prohibits the placing on the EU market, putting into service, or use of certain AI systems for practices of manipulation, exploitation, social control, or surveillance, which by their nature violate fundamental rights and the values of the Union. In particular, such systems infringe human dignity, freedom, equality, democracy, and the rule of law, as well as fundamental rights enshrined in the Charter of Fundamental Rights of the EU (CFREU), including, among others, the right to non-discrimination (Article 21), equality before the law (Article 20), data protection (Article 8), respect for private and family life (Article 7), the rights of the child (Article 24), freedom of expression (Article 11), the right to an effective remedy and to a fair trial (Article 47), and the presumption of innocence and the right of defence (Article 48).

The AI Act does not provide a precise definition of subliminal techniques, but these are understood as techniques that impair awareness and influence the behaviour of individuals interacting with the AI system. Practical examples include subliminal visual or auditory messages, hidden images embedded among other visual content that are unconsciously processed by individuals and influence their behaviour. Another example is diversion, where the AI system draws the user's attention to specific content in order to conceal other content, exploiting cognitive biases and vulnerabilities in attention (e.g., influencing consumer purchasing choices). The manipulation of time perception, which can induce anxiety and dependence, is another such example.

Deliberately manipulative techniques are designed to influence, alter, or control individual behaviour in ways that undermine autonomy and freedom of choice. A practical example is sensory manipulation, where AI systems provide an audiovisual background that alters mood, causing anxiety and stress, and influencing user behaviour to the point of causing significant harm. Such manipulative techniques can be personalised when AI systems generate persuasive messages based on individuals' personal data or exploit their specific vulnerabilities. Some AI systems may not have been developed with manipulative intent, yet may still apply these techniques based on the datasets on which they were trained. For this prohibition to apply, all the conditions set out in the provision must be met cumulatively.

Deceptive techniques may consist in the presentation of false or misleading information with the aim, or even the effect, of deceiving individuals and influencing their behaviour in ways that compromise their autonomy, decision-making process, and freedom of choice. Practical examples include intelligent chatbots that impersonate an acquaintance or relative using synthetic voice in order to carry out scams or cause significant harm; AI systems that learn to identify moments of evaluation and control and 'hide' dangerous behaviours for as long as necessary.

Significant harm may include stress, anxiety, insomnia, addiction, self-harm, exacerbation of stalking, cyberbullying, harassment, incitement to hatred and violence against certain minorities, or psychological harm resulting from identification with victimised groups through deepfake techniques.

With regard to the placing on the market, putting into service, or use of AI

systems that exploit the vulnerabilities of individuals or specific groups, the AI Act does not provide a precise definition of vulnerability – a concept that can encompass a wide range of types, including cognitive, emotional, physical, and other forms of fragility that may affect an individual's or a group's ability to make informed decisions or, more generally, their behaviour. However, the Regulation expressly prohibits AI practices that may exploit vulnerabilities arising from certain factors such as age, disability, or specific socio-economic situations, which generally make it more difficult to recognise or resist manipulative or distortive AI practices.

For this prohibition to apply, all the conditions set out must be met simultaneously, including, in particular, a plausible causal link between the exploitation, the distortion of the behaviour of the person interacting with the AI system, and the significant harm that has resulted or can reasonably be expected to result.

With regard to age, the vulnerable groups identified include both minors and older people. Minors are particularly sensitive to manipulative techniques because their stage of development limits their ability to critically assess what is real and the intentions behind AI-driven interactions. Owing to their general immaturity, minors are especially susceptible to the risk of developing forms of dependency on artificial agents and AI-based applications.

Examples include smart toys that encourage children to engage in dangerous actions by turning them into challenges to be won in exchange for digital rewards; certain video games capable of analysing children's behaviour and preferences and, on that basis, creating personalised digital rewards that may induce addiction, stress, and other significant and long-term consequences such as insomnia, myopia, concentration difficulties, social and relational difficulties, eating disorders, depression, and self-harm. AI systems may also be used for the generation of child sexual abuse material and the development of strategies for grooming minors. However, not all types of smart toys, video games, or educational applications are generally prohibited – only those that exploit minors' vulnerabilities and may cause them significant harm.

Older people may experience reduced cognitive abilities (not necessarily due to dementia) and may have difficulty using and interacting with AI systems because of limited digital skills, making them particularly susceptible to scams and manipulative marketing strategies. The harm is often financial and psychological, and is frequently exacerbated by conditions of isolation. Examples include AI systems that exploit the vulnerabilities of older people by advertising expensive medical treatments, unnecessary insurance, or deceptive investment schemes that lead to loss of savings, increased debt, and stress. These systems often take advantage of the specific socio-economic situations in which older people find themselves. Other examples include caregiver robots that may exploit the fragility of those they care for and coerce them into activities against their will, worsening their mental and physical health. Not all such applications are prohibited – only those that exploit vulnerabilities and cause or are likely to cause significant harm.

Article 5 of the AI Act also aims to prevent the risk that AI systems may exploit the limitations and vulnerabilities of persons with disabilities and to protect them from harmful influences and manipulative practices. The concept

of disability encompasses a wide range of long-term physical, mental, intellectual, and sensory impairments which, in interaction with various barriers, hinder the full and effective participation of individuals in society on an equal basis with others (see UN Convention on the Rights of Persons with Disabilities). Persons with disabilities may be more easily influenced and exploited than others. Examples include: a therapeutic chatbot intended to provide daily support and strategies for persons with mental disabilities but which may exploit their limited intellectual abilities to influence them into purchasing expensive devices and medical products that promise unrealistic benefits, or condition them to the point of adopting behaviours that are dangerous to themselves or others. Certain AI systems may identify women and girls with disabilities online in order to use them to generate pornographic content or to develop more effective grooming practices. With regard to specific social and economic situations, the term 'specific' does not refer so much to an individual characteristic as to a particular legal status or membership of a specific vulnerable social or economic group.

According to Recital 29, this group may include persons living in conditions of extreme poverty, as well as members of ethnic and religious minorities. The category covers not only relatively stable and long-term situations, but also temporary circumstances such as short-term unemployment, over-indebtedness, and migrant status. Persons in such conditions are typically particularly vulnerable, have few resources, and possess limited digital skills compared to the rest of the population, which makes it more difficult for them to recognise and resist manipulative AI practices. An example would be a predictive AI algorithm used in targeted advertising strategies for predatory financial products aimed at people living in low-income areas who are in precarious financial situations, exploiting their desperation.

AI systems that exploit socio-economic data could disproportionately affect ethnic minorities or individuals belonging to a particular ethnicity, exacerbating existing disparities and contributing to forms of systemic discrimination and even to the exclusion of individuals from those groups. However, the AI Act does not apply to systems that target consumers based on a wide range of variables that are not directly linked to vulnerable groups in specific socio-economic situations (such as smartphone use, the size of the city in which they live, or their travel destinations and frequency). Certain AI chatbots, for example, could push migrants or refugees – who often lack a clearly defined legal status and stable socio-economic conditions – towards extremist positions and incite hatred and violence against certain population groups by exploiting their particular sensitivity to specific content and fear-based narratives.

4.1.2 High-risk AI systems.

The type of systems most thoroughly regulated are those categorized as "high-risk". A system is classified as such under Article 6 of the AI Act if two conditions are met:

- It is intended to be used as a component of safety in a product, or it is itself a product, in both cases governed by the regulations in Annex I.
- The AI system (whether as a safety component or as a product) is subject

to third-party conformity assessment for market placement or deployment, according to the regulations in Annex I.

The conformity assessment (under Article 43) referred to in Article 6, paragraph 1, letter b, relates to the system's compliance with the requirements set out in Articles 8 and following: the presence of a risk management system (under Article 9) and appropriate technical documentation (under Article 11), the need for human oversight (under Article 14) and specific transparency obligations for deployers (under Article 13), as well as inherent characteristics of the system such as its accuracy, robustness, and cybersecurity (under Article 15), data quality, and data governance (under Article 10).

At the same time, AI systems listed in Annex III are also considered high-risk, namely those operating in the areas of:

- Biometric identification
- Management and maintenance of critical infrastructure
- Access to education or evaluation of educational pathways
- Selection of candidates or management of employment relationships
- Access to essential public or private services
- Systems used by law enforcement, if permitted under Union and national law
- Control of migration phenomena, asylum requests, and border control, if authorized by Union and national law
- Administration of justice and democratic processes

However, AI systems listed in Annex III may be considered not high-risk if they do not present a significant risk of harm to health, safety, or fundamental rights, even in the sense of not materially influencing the outcome of the decision-making process. It should be noted that if a system in Annex III involves the profiling of individuals, it is always considered high-risk.

4.2 General Purpose AI Models.

Regarding AGI, the AI Act regulates GenAI starting from its foundations, namely the so-called general-purpose models (GPAI - General Purpose AI models). Given their ability to serve multiple purposes, fundamental models have become one of the key topics in European AI regulation, particularly following the advent of Chat-GPT, and have been categorized into two groups:

- Systemic models
- Generic models

Both types of models are capable of performing a range of operations, but while the latter are considered to have greater safety, the former are characterized by their so-called high impact capability. For this reason, increasing obligations have been foreseen between generic and systemic GPAI models, with more stringent requirements for general-purpose AI models with systemic risk, as these may expose the European market and the foundational values of the EU to so-called systemic risks (Fig. 6).

There are numerous references to the regulation of the DSA (Digital Services Act), both in terms of the scale of AI and the definition of systemic risk. Indeed, there is a presumption of "high impact capability" when the total computing power used for training the AI model exceeds 10^25 FLOPs, although this can

be surpassed by the European Commission. The adopted approach grants the Commission significant discretionary power, both within the system for defining and governing Artificial Intelligence, including the designation of models as "systemically risky" and modifying the definition under changing conditions, as well as overseeing all general-purpose AI models, as the Commission holds exclusive competence under Article 88 of the AI Act.

Level of risk	Discipline
Systemic risk - AI models for general purpose systemic risk (Systemic models)	- Particularly detailed transparency obligations (Art. 53) - More intrusive obligations (Art. 55) - Burden of codes of good practice (Art. 56)
Limited risk – General purpose AI models (Generic models)	- Particularly detailed transparency obligations (Art. 53) - Burden of codes of good practice (Art. 56)
Minimal Risk - Certain General Purpose AI Systems	- Transparency obligations (Art. 50) - Burden of codes of good practice (Art. 56) - Burden of codes of conduct (Art. 95)

Fig. 6

4.2.1 Systemic AI Models.

For systemic GPAI models, not only are the same detailed transparency obligations applied as for generic models, but also an additional set of requirements due to the identified criticalities. These further obligations are set forth in Article 55 and carry a more intrusive nature:

- Compliance evaluation of the model with standardized protocols reflecting the state of the art, including the documentation of adversarial tests to identify and mitigate systemic risks;
- Assessment and mitigation of potential systemic risks at the Union level, including related causes such as the development, market placement, or use of general-purpose AI models with systemic risk;
- Tracking, documenting, and reporting – without undue delay – to the AI Office and, when appropriate, to the relevant national authorities – pertinent information about serious incidents and potential corrective measures to address them;
- Ensuring an adequate level of cybersecurity protection regarding the model and its physical infrastructure.

To demonstrate compliance with the above obligations, suppliers of GPAI models can rely on codes of good practices under Article 56.

4.2.2 Generic AI Models.

In regard to the regulation of generic GPAI models, detailed transparency obligations are established under Article 53, such as the requirement to prepare technical documentation that makes the model's functioning understandable, including the training and testing process. This documentation must be provided to those intending to integrate the model into their AI systems and, upon request, to the AI Office. At the same time, a policy must be in place to protect intellectual property rights, and a summary

of the content used during training must be made publicly available. The adoption of codes of good practices under Article 56 is also required, just as for systemic models.

Particular attention is given to GPAI models released under open-source licenses, which allow access, use, modification, and distribution of the model, with parameters – including weights, model architecture, and usage information – made public. In this case, providers are subject to fewer obligations unless the models present systemic risks.

Generative Artificial Intelligences (GenAI) are revolutionizing how people live and work. While human oversight has always been deemed essential in the AI field, it takes on a primary role in the context of information: technology renews information, but risks multiply, making it crucial that automatically generated content is clearly recognisable and not confused with conventionally generated content.[20]

In the legal field, this shift has led legal practitioners – including judges, lawyers, and legal scholars – to acquire digital skills for using new tools. These tools can now be delegated not only for drafting legal documents but even part of decision-making processes (Decision Support Systems, DSS). One example of a GenAI system is Microsoft's CoPilot chatbot, which can be used to draft legal act drafts using document models from the personal computer's memory or by retrieving large amounts of text from the web. While this is not a system specialized in the legal field, it reflects a new configuration of legal information, necessitating a change in cultural paradigms. The true revolution of these new intelligent systems lies in their potential to support legal reasoning. An Italian experiment in this regard is Giurimatrix, an AI system specialized for the legal sector developed by Professor Filippelli and Lawyer Viola.

The use of these programs, however, must be accompanied by an awareness of their fallibility and the need for digital literacy among professionals in all fields, not just in law. This awareness was achieved in the legal sector during the G7 for Lawyers organized by the CNF on April 16 2024.[21] For ensuring AI reliability in these contexts, the following ten actions are deemed indispensable:

1. Create a task force to conduct a survey to collect data on the state of the art regarding AI applications in law firms and their purposes.
2. Assess compliance with privacy regulations and the level of data digitization.
3. Identify the normative principles (e.g., ethical code) considered essential for the legal profession's identity.
4. Develop an assessment tool for AI tools based on the above principles.
5. Certify AI tools used in legal practice under the EU AI Regulation, with particular attention to the FRIA (Fundamental Rights Impact Assessment) procedure (Article 27 and Annex III).
6. Adapt all procedural acts (including those of judges) to the criteria of Ministry of Justice Decree no. 110 of 2023, enabling their use in training AI tools.

[20] G Corasaniti, *Tecnologie intelligenti: Rischi e regole* (Mondadori Università 2023) 38.
[21] L Gatt, '10 azioni per sviluppare la IA in Italia' (2024) 2 La Nuova Procedura Civile.

7. Standardize legal procedural acts and information for AI training: configuring uniform legal data that can be understood by different systems.
8. Provide intensive and thorough training for lawyers on the conscious and critical use of AI tools.
9. Create a basic AI tool shared with various functions (both drafting and legal reasoning – "Algorithm 12").
10. Ensure interoperability of all AI tools in the legal field with those used by judicial bodies and public administrations.

On a broader scale, GenAI raises complex regulatory issues due to its transition from processing linguistic models to processing world models. Whereas GenAI previously only understood syntax and grammar, this new alien manufactured[22] is now making the leap toward understanding meaning. This introduces new demands for legal mediation, prompting legislators, particularly in the EU, to consider whether «regulation or liability»[23] is the most appropriate protective tool, with further training needed for operators downstream.[24] In this context, it becomes necessary to speak of the intelligent use of smart technologies as the best means to detect and counteract the drifts of planned marginalisation.[25]

4.2.3 Certain AI systems.

With the advent of general-purpose AI models, the AI Act also regulates cases where these models form the basis of AI systems. This involves the so-called 'general-purpose AI systems', which, being based on general-purpose AI models, have the capability to pursue various objectives.

In light of this, for certain general-purpose AI systems and basic AI systems (i.e., non 'general-purpose'), the Union legislator has identified transparency obligations. According to Article 50:

- When basic AI systems interact directly with natural persons, they must be designed and developed in such a way that individuals are informed they are interacting with AI. The only exception to this rule is when it is clearly evident, taking into account the moment and context, that the interaction involves an AI system.
- When AI systems – both "general-purpose" and basic – generate synthetic content (audio, video, images, or texts created or modified by AI), the outputs must be marked in a readable format and identified as artificially generated or manipulated. The exception applies to AI systems that perform standard editing functions or do not substantially alter the input data provided by the deployer or its semantics, or if authorized by law for detecting, preventing, investigating, or prosecuting crimes.

[22] U Ruffolo, 'Intelligenza Artificiale generativa e mediazione giuridica', conference speech at Stati Generali del Diritto di Internet e della Intelligenza Artificiale on the 28, 29, 30 november 2024. <https://www.youtube.com/watch?v=aKylH1Zm2Hw>.
[23] Ruffolo (n 22).
[24] Corasaniti (n 20) 42.
[25] Corasaniti (n 20) 39. The author makes a warning: it is necessary for law, economics and technology to come together in order to identify the best actions to exploit the full potential of information and to counter illegal activities.

- In reference to emotion recognition systems or biometric categorization systems, individuals must be informed of the system's functioning, and these systems must handle personal data in compliance with Regulation (EU) 2016/679, [26] Regulation (EU) 2018/1725, [27] and Directive (EU) 2016/680,[28] depending on the case.
- For AI systems generating or manipulating deep fakes, it is necessary to disclose that the content has been generated or manipulated artificially (digital watermark). The exception applies when the use is authorized by law for detecting, preventing, investigating, or prosecuting crimes.
- For AI systems generating or manipulating texts published to inform the public on matters of public interest, it must be disclosed that the text has been generated or manipulated artificially. The exception applies when the use is authorized by law for detecting, preventing, investigating, or prosecuting crimes, or if the AI-generated content has undergone human review or editorial oversight, and a natural or legal person holds editorial responsibility for the publication of the content.

Additionally, these systems have the burden of adopting codes of conduct (art. 95) and code of good practices (art. 56).

To conclude, the final risk pyramid of the AI Act, when assessed in its entirety, appears as follows (Fig. 7).

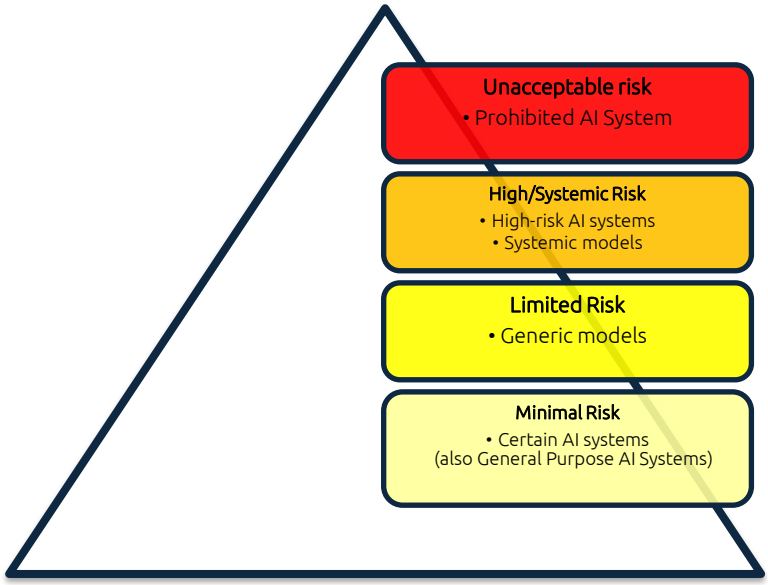


Fig. 7

[26] Parliament and Council Regulation 2016/679/UE of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR) [2016] OJ L119/1. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>.

[27] Parliament and Council Regulation 2018/1725/UE of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39. <https://eur-lex.europa.eu/eli/reg/2018/1725/oj/eng>.

[28] Parliament and Council Directive 2016/680/UE of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L11/89. <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>.

5. FRIA - Fundamental Rights Impact Assessment.

In the field of AI, particular importance is attached to the Fundamental Rights Impact Assessment (FRIA) for high-risk AI systems under Article 27 of the AI Act. This activity involves measuring the impact of high-risk AI systems on fundamental rights with a view to ex-ante protection, following a risk-based approach. By assessing the potential risks of harm arising from the application of AI, it functions as a true tool of accountability.[29]

As previously mentioned, this activity is only mandatory for certain deployers: for those of high-risk systems under Article 6, Paragraph 2 of the AI Act – that is, the AI systems listed in Annex III, except those intended for use in the sectors outlined in point 2 – for public organizations or private entities providing public services, and for deployers of high-risk AI systems listed in Annex III, point 5, letters b) and c) (i.e., those related to creditworthiness assessments and the determination of risks and prices in the life and health insurance sectors).

Preliminary elements to the Fundamental Rights Impact Assessment (FRIA) are undoubtedly those AI impact measurement models developed by supranational institutions. One example is the ALTAI (Assessment List for Trustworthy Artificial Intelligence), a tool that, based on the Ethical Guidelines for Trustworthy Artificial Intelligence presented by the High-Level Expert Group on AI (AI HLEG) to the European Commission in April 2019, supports the implementation of the key requirements outlined in those guidelines. From the reading of the Ethical Guidelines[30], it is evident that the necessary components to define a trustworthy AI system are three:

- Legality (the system must comply with all applicable laws and regulations);
- Ethicality (the system must adhere to shared ethical principles and values);
- Robustness (both technical and social, to minimize the risk of unintentional harm).

At the same time, seven requirements have been highlighted that AI systems must meet throughout their lifecycle to be considered trustworthy:

- Human intervention and oversight (including the respect of fundamental rights, human intervention, and human oversight);
- Technical robustness and security (including resilience to attacks, emergency planning, general security, accuracy, reliability, and reproducibility);
- Data privacy and governance (including data confidentiality, quality, integrity, and access);
- Transparency (including traceability, explainability, and communication);
- Diversity, non-discrimination, and fairness (including the prevention of unfair biases, accessibility, universal design, and stakeholder

[29] L Gatt and others, 'FRIA Implementation Model According to the AI Act' (2024) IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), 1224-1229. <https://ieeexplore.ieee.org/document/10796624>.

[30] AI HLEG, 'Ethics guidelines for trustworthy AI' (2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

participation);
- Social and environmental well-being (including sustainability, environmental respect, social impact, society, democracy, and collective interests);
- Accountability (including verifiability, minimization of negative effects, and reporting, trade-offs, and remedies).

Operationally, through the Assessment List for Trustworthy AI (ALTAI), the principles of AI are translated into an accessible and dynamic checklist that guides AI developers and distributors in the practical implementation of these principles, creating a self-assessment tool.[31] In the same vein and with the same self-assessment approach, the European Commission for the Efficiency of Justice of the Council of Europe (CEPEJ) developed in 2023 an evaluation tool for the operationalization of the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. This self-assessment tool,[32] which refers to the principles outlined in the Ethical Charter adopted in December 2018,[33] proposes a questionnaire based on 29 questions to provide clear, practical guidance on how to concretely apply the Charter. Furthermore, this tool seems to complement the Human Rights, Democracy, and Rule of Law Impact Assessment (HUDERIA) presented by the Committee on Artificial Intelligence (CAI) of the Council of Europe during its 12th plenary session in November 2024.[34]

At the same time, significant contributions to the development of these tools have also come from other actors: such as Mantelero's studies,[35] ALIGNER Fundamental Rights Impact Assessment (AFRIA),[36] the FRAIA tool developed by the Dutch Government,[37] research presented by the Intesa Sanpaolo team,[38] or proposed solutions for improving AI fairness.[39]

Despite being based on excellent premises, these tools are not yet fully

---

[31] AI HLEG, 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment' (2020) <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.

[32] CEPEJ, 'Assessment Tool for the Operationalisation of the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment' (2023) <https://rm.coe.int/cepej-2023-16final-operationalisation-ai-ethical-charter-en/1680adcc9c>.

[33] CEPEJ, 'European ethical Charter on the use of Artificial Intelligence in judicial system and their environment' (2018) <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

[34] CAI, 'Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (HUDERIA methodology)' (2024) <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f>.

[35] A Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template' (2024) 54(106020) CLSR <https://www.sciencedirect.com/science/article/pii/S0267364924000864>.

[36] Aligner, 'ALIGNER Fundamental Rights Impact Assessment (AFRIA)' (2020) <https://aligner-h2020.eu/>.

[37] Government of Netherlands, 'Impact Assessment Fundamental Rights and Algorithms' (2022) <https://www.government.nl/documents/reports/2022/03/31/impact-assessment-fundamental-rights-and-algorithms>.

[38] S Bertaina and others, 'Fundamental Rights and Artificial Intelligence Impact Assessment: A New Quantitative Methodology in the Upcoming Era of Ai Act' (2025) 56(106101) CLSR. <https://www.sciencedirect.com/science/article/pii/S0267364924001663>.

[39] A Calvi, D Kotzinos, 'Enhancing AI fairness through impact assessment in the European Union: a legal and computer science perspective' in FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, 2023, 1229–1245. <https://dl.acm.org/doi/abs/10.1145/3593013.3594076>.

comprehensive for ensuring the anticipated preventive protection: these systems do not provide an overarching view of fundamental rights but rather focus on specific aspects, and a complete analysis is lacking, which is necessary to ensure the effective protection of individuals, especially in specific application contexts. In this context, due to the absence of an effective tool suited to evaluating the impact of AI on fundamental rights in a quantifiable, automatic, and objective manner, assessment errors could occur, potentially leading to excessive or unexpected costs for individuals and businesses.[40]

The difficulties that legislators face in developing tools to prevent and measure the negative impacts of new technologies on fundamental rights stem primarily from the fact that the so-called fourth digital revolution[41] and the social implementation of AI in all fields have placed contemporary society in a condition, described by Anders as characteristic of the technical man, of a Promethean gap, [42] such that we are no longer able to control our own technological actions, neither morally nor cognitively. This condition translates into a *de iure condendo* framework where the relationship between new technologies and law resembles the relationship between the hare and the tortoise, forcing regulation to set fixed points while also continuously updating them to the evolving AI systems that are the subject of legislative action. This creates the risk of legislative hypertrophy, leading to ever-decreasing legal certainty. The most vulnerable groups, both as individuals and as communities (the elderly, people with disabilities, minors, digital illiterates in general), are particularly affected by this situation, as they are most exposed to the risk of digital alienation of their rights and the erosion of social protection mediated by the law.

In this context, a critical issue that the legislator faces, within the framework of an inescapable need for an ethical approach to AI, is the feasibility of developing machine-readable ethical principles to be embedded within AI systems – an "ethical language" that machines could manage independently, thereby potentially relieving AI producers and operators from legal responsibility or redistributing such responsibilities in a more advantageous manner.

In this regard, although central to a digital ethics, modern technology makes the traditional concept of ethics insufficient. [43] In this view, Benanti and Maffettone [44] recognizing the criticality of a simplistic association between traditional ethics and the moral dilemmas posed by new technologies, argue that it would be wrong to think that it is possible to implement moral theories in AI systems if ethics is understood as the human competence to consciously discern what is right or wrong in a defined context of choice regarding the pursued ends or the consequences of one's actions. The algorithm cannot possess ethical capability, but it can – and must – be ethically designed.

[40] L Gatt and others, 'FRIA Implementation Model According to the AI Act' (2024) IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), 1224-1229. <https://ieeexplore.ieee.org/document/10796624>.
[41] L Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (Raffaello Cortina editore 2017).
[42] G Anders, *L'uomo è antiquato. I. Considerazioni sull'anima nell'epoca della seconda rivoluzione industriale*, trad. L. Dallapiccola (Bollati Boringhieri 2007).
[43] Portinaro (n 7) XXII.
[44] P Benanti, S Maffettone, *Noi e la macchina* (Luiss University Press 2024).

Algorithmetica, if we use this term to refer to the ethical reflection applied to the engineering of the algorithm, must be nothing more than this precautionary and responsibility-based principle in its design. There cannot be an ethics of the algorithm in the sense of a language, a moral competence that it can handle on its own, as one of the possibilities of a generative AI. The ethicality of the algorithm can only translate into an ethics-by-design approach by human operators who program the machines while being aware of the risks involved in implementing AI across various operational environments with social impact.

In a vision of trustworthy and ethical AI,[45] the choice of an applicable ethical theory, whatever it may be, must take into account the fact that relevant rights may conflict with each other (e.g., security and privacy regarding biometric data processing) and that not all human beings share the same values.

However, there are two concepts that, according to Benanti and Maffettone, remain constant, regardless of the ethical theory of reference: justification and value. First, any moral judgment must be justified. To do this, the agent who expresses the judgment indicates a norm that may not be shared by the reference community. From there, the agent refers to a moral principle – which in turn is based on a value – and ultimately to the chosen ethical theory. In this sense, justification and value are interconnected.

The challenge then lies in defining what values are considered relevant in the face of the risks of the digital revolution and why.

There are two manifestations of value that we experience daily: self-realization (leading a morally worthy life achieves the well-being of each individual) and respect (every human being recognizes the limits of their freedom in that of others). The ethical theory that best combines both forms, according to the two authors, is one that views value as an organic unity, where a surplus of value is realized when the value of the whole exceeds that of the sum of its individual parts.[46] This interpretation of value implies recognizing an objective – not just subjective – value for certain behaviors. Thus, we can say that human beings choose how to behave after resolving the tension between their moral actions as individuals and as members of a community, whatever that community may be. What must not be lost sight of, therefore, is the centrality of the human being, both generally and specifically in the governance of new machines that transition from being automatic to increasingly autonomous.

In conclusion, if it is true that ethics cannot be applied like engineering, regulation must address all use cases of AI systems that could negatively impact fundamental rights and therefore pose moral dilemmas (e.g., autonomous machines and aircraft, drones used for military purposes, etc.). This is the socio-technological character of AI: it loses its apparent neutrality in its practical applications.

If one were to apply the general theory that sees value as an organic unity to specific problematic cases, the following steps should be taken:[47]

---

[45] AI HLEG, 'Ethics guidelines for trustworthy AI' (2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
[46] Benanti, Maffettone (n 44) 88.
[47] Benanti, Maffettone (n 44) 91.

1. Carefully describe the case in question;
2. Explicitly identify how the facts affect shared values;
3. Know who is involved and who has a moral right in the case;
4. Highlight the foreseeable consequences of a particular decision;
5. Understand the relationships between the people involved and the foreseeable consequences of the choice made on them;
6. Opt for the choice linked to the maximum value in terms of organic unity.

What the two authors actually propose is the recourse to an ethical theory of value as an organic unity, in whose application the moral, social, and legal situation is crucial.

Addressing the issue of ethics for the digital realm is imperative: technological artifacts in general, and particularly computer algorithms, have caused an anthropological shock such that they delineate new hierarchies of values (for example, the conception of the common good changes), create new needs, and even radically transform the perception that humans have of themselves and the world in which they live. This condition inevitably has consequences for the moral actions of human beings. Hence the need to identify the ethical principles that the design and use of AI systems should be inspired by, taking into account the possible impacts these systems may have on politics, the economy, and law.

Any discourse on algorethicality begins with the need to rethink subjectivity as no longer individual, as a privileged prerogative of single human actors:[48] the human being who cooperates in their moral actions with non-human subjectivities is defined as *homo algorithmus.*[49] Within this reciprocal influence, it is necessary to identify ethical principles that can be shared by both components of the newly formed subjectivity. The fundamental ethical norm is the protection of human dignity, from which a series of principles descend: intuition, intelligibility, and adaptability.

First, the algorithm must be capable of perceiving human intentions and adapting accordingly. This is made possible by machine learning and, therefore, by human experience. The principle of intelligibility implies that humans must be able to intuit the action the algorithm will perform. Thus, it must be transparent and traceable, meaning that humans should be able to understand the underlying logic that led the AI system to produce a certain output based on input data, and this information must always be accessible to avoid the opacity (black box) typical of more complex AI systems. Finally, the adaptability of the algorithm to human intentions stems from the ability of the technological artifact to relate to its human counterpart, whether programmer or user.

A moral choice generally involves three elements: awareness, freedom, and responsibility. [50] The intelligence attributed to artificial entities does not correspond to human intelligence: the former is capable of finding solutions to specific problems, while the latter is of a general type. Thus, the algorithm may

[48] C Accotto, *Il mondo dato: cinque brevi lezioni di filosofia digitale* (Egea 2017) 93.
[49] A Picchiarelli, 'L'algoretica e lo sviluppo etico dell'Intelligenza Artificiale' in R. Razzante (ed.), *Manuale sull'Intelligenza Artificiale* (Giappichelli Editore 2024).
[50] Picchiarelli (n 49).

only have practical awareness related to the specific problem it addresses and for which it was created.

The freedom that leads humans to perform moral actions is influenced by the new filter between the agent and the world, represented by the algorithm: new technologies have exponentially increased human capabilities, but with unpredictable outcomes. This leads to a concept of uncertain collaboration (uncertainty) between humans and algorithms.[51]

Regarding the concept of responsibility, since moral action is the result of cooperation between multiple agents – human and non-human – some philosophers have used the concept of distributed responsibility. All moral agents are accountable for their actions, but they are not always considered responsible:[52] in the event of damage caused by an algorithmic system used by a human, it is not appropriate to speak of full responsibility on the part of the artificial agent but rather of accountability (attribution) for the effect of the influence the algorithm has on the human agent.

To avoid technocratic developments, where technologies – or rather, those who govern them – determine the relevant values rather than communities, and to achieve authentically anthropocentric technological development, an interdisciplinary approach is necessary. This approach should develop governance frameworks that ensure collaboration between humans and algorithms according to the human-in-the-loop paradigm.

Although from different perspectives, both Benanti and Maffettone, and Picchiarelli, question the possibility of applying moral categories to artificial agents and the need to develop a new ethics that is not a replacement but an integrative extension of traditional ethics.

A measured and measurable law seems clearly possible, but it is essential to follow the digital innovative path that scholars are committed to design, as scales, values, and norms serve as closure elements of the law and guide its related outcomes.[53]

At the same time, just as there is an increasing need to valorize a decision-making method that is humanly verifiable in terms of logic, controllability, and justification,[54] there is an ever-stronger demand to monitor the impact of artificial intelligence models on equity.

Social equity proves to be a concept of significant complexity: it is necessary to consider the various applications of AI, capture the different types of damage it could potentially cause, and reflect the perspectives of different existing communities. On this point, although simple rankings were relied upon for a long time to assess the potential damage to various communities, more recently, the need for a more comprehensive approach has emerged: shifting from AI equity rankings, which attempt to reduce equity to a single number, to a comprehensive suite of benchmarks that perform a variety of measurements and can provide tools to understand both the broad range of potential harms and trade-offs between different aspects of equity.[55]

---

[51] Picchiarelli (n 49).
[52] Picchiarelli (n 49) 8.
[53] G Corasaniti, *Informatica giuridica e progettazione innovativa digitale* (Cedam 2024) 185.
[54] Corasaniti (n 53) 187.
[55] A Wang, A Hertzmann, O Russakovsky, 'Benchmark suites instead of leaderboards for evaluating AI fairness' (2024) 5 (11) Patterns. <https://www.cell.com/patterns/fulltext/S2666-3899(24)00239-3>.

5.1 Possible new developments.

It is indisputable that the FRIA (Fundamental Rights Impact Assessment) in its current state presents limitations: the AI Act alone is insufficient to specify how to effectively implement a FRIA, as it does not provide the parameters for creating appropriate measurement pathways.[56] Instead, it only includes a generic reference to Article 27, paragraph 5, regarding the preparation by the AI Office of a 'template for a questionnaire, including through an automated tool, to facilitate deployers in complying with their obligations'. At the same time, there is an increasing need for an assessment conducted by public and impartial bodies acting as true certifying entities for AI that respects fundamental rights.

It is precisely in this context that the project born from the collaboration between the Research Centre ReCEPL (Research Centre in European Private Law),[57] CNF (National Forensic Council)[58] and CNR-Isti (National Research Council - Institute of Science and Technology for Information "Alessandro Faedo"),[59] the FRIA Project, is positioned.

The partnership project, in which the CNR-Isti has been replaced by the HABES research laboratory (Hardware Assisted and Blockchain Empowered Security lab)[60] and the CoLAB-AI Observatory, in addition to the typical challenges of complex legislation, however, presents a further challenge, this one not only of a technical nature: it is indeed essential to establish a shared methodological approach that allows for effective collaboration both among the project's various partners and with the public authorities, both Italian and European, some of which are still in the process of consolidation.

The multidisciplinary team is working on a project to assess the impact that artificial intelligence systems can have on the fundamental rights of individuals, with the aim of developing a tool capable of semi-automatically identifying the risks associated with the use of these technologies. The ultimate goal is to provide a tool that ensures effective, rigorous, and timely analysis, fully compliant with the complex regulatory framework currently in place regarding artificial intelligence.

This is, therefore, an initiative that requires not only high-level legal and scientific expertise but also an interdisciplinary and collaborative approach, aimed at building a concrete and productive dialogue between research and various institutions, in order to jointly address the regulation of artificial intelligence and the protection of fundamental rights – issues that are as complex as they are important.

---

[56] L Gatt and others 'FRIA Implementation Model According to the AI Act' (2024) IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), 1224-1229. <https://ieeexplore.ieee.org/document/10796624>.
[57] RECEPL - Research Centre in European Private Law. <https://www.unisob.na.it/ateneo/c008.htm?vr=3>.
[58] CNF - Consiglio Nazionale Forense. <https://www.consiglionazionaleforense.it/>.
[59] CNR-Isti - Consiglio Nazionale delle Ricerche - Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo". <https://www.isti.cnr.it/it/>.
[60] HABES Lab - Hardware Assisted and Blockchain Empowered Security lab. <https://habes.cs.unisa.it/>.

6. Conclusions.

It was difficult to imagine that on May 30, 2023, a statement of this kind would come from the upper echelons of digital technocracy: 'AI could lead to the extinction of humanity'. This alarm was raised by AI gurus such as Sam Altman (ChatGPT OpenAI), Demis Hassabis (Google DeepMind), and Dario Amodei (Anthropic), following some hearings in the US Congress on AI, Elon Musk's call for a moratorium on AI research to assess its risks and social impact, and a contribution by Yuval Harari on The Economist, where he argued that by taking control of language in general in our increasingly mediated society, AI has essentially "hacked" the operating system of our civilization. These concerns thus reached the general public, beyond the specialized debate.

This makes even more urgent the question underlying this contribution on what we can expect from AI in the coming years, after the first European law on the matter. A question that challenges the common narrative about AI, according to which the US develops the technology, China copies it, and Europe limits itself to regulating it. This argument is often used to push the European Union and its Member States to invest more in the development of AI systems in order to position themselves credibly within the strategies of major private and public players on an international scale, but it risks undermining the systemic scope – and the global momentum – of the importance of regulating AI implementation in the maturing digital society. It is now a regulatory request even from the Big Tech companies themselves, and it is absolutely decisive in order to ensure not only the overall well-being of society, with an anthropocentric use of AI, but specifically the fundamental rights of individuals, not only as single individuals but as members of a social community.

In response to this regulatory need, since 2020 – with the European Commission's Communication A European Strategy for Data[61] – the European Union has expressed its ambition to become a global benchmark for the regulation of new technologies and data governance. Unlike the U.S. and Chinese models – which respectively entail a high concentration of data space management by the private sector, and a combination of state surveillance and control by Big Tech – the European Union proposes a third way for regulating the processing of data essential to the development of AI models. This approach seeks to reconcile the legitimate interest in collecting, processing, and using data with the protection of fundamental rights. This model translates into the creation of a single data market through the establishment of European data spaces, the enhancement of computing infrastructure, the promotion of data portability and sharing, and the development of digital skills. The Continent Action Plan[62] of 9 April represents a further step in the European political strategy aimed at pursuing a 'third way' compared to the U.S. and Chinese models mentioned above. In this communication, the Commission

[61] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Strategy for data, Brussels, 19.2.2020, COM (2020) 66 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.

[62] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "AI Continent Action Plan", Brussels, 9.4.2025, COM (2025) 165 final. <https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=COM:2025:165:FIN>.

reiterates the Union's ambition to become a global leader in artificial intelligence, while ensuring its development remains human-centred and trustworthy. This objective is to be achieved through concrete actions along five main lines: enhancing computing infrastructure; ensuring greater access to high-quality data; developing AI algorithms and increasing their application in strategic sectors; strengthening digital literacy at all levels of the population; and optimising single market regulation to improve regulatory compliance.

Within the Union, computing capacity – which is essential for the development of AI models throughout their entire life cycle – is made accessible through the network of cutting-edge European supercomputers coordinated by the European High-Performance Computing Joint Undertaking (EuroHPC), such as LUMI, Leonardo, and MareNostrum. This partnership provides substantial resources to start-ups, industry, public administrations, and researchers, enabling broad participation in the development of state-of-the-art AI models.

The EuroHPC has recently been enhanced through the AI Innovation Package (2024), which provides for the creation of AI Factories – currently thirteen – designed to foster innovation, cross-sector collaboration, and the application of new models in strategic areas such as health, technology, the environment, education, industry, finance, agriculture, cybersecurity, space, and the public sector. These infrastructures are open to participation by EU Member States and associated third countries, which may establish AI Factory Antennas to provide remote access to the supercomputing resources of the corresponding AI Factory located in another Member State.

The EuroHPC will serve as a single point of access to the support services offered by the AI Factories for users across Europe, particularly start-ups, SMEs, and EU-funded research projects, ensuring streamlined access to computational resources while reducing administrative costs. The next step will be the establishment of AI Gigafactories – large-scale infrastructures dedicated to the development and training of next-generation AI models with trillions of parameters. To this end, these infrastructures will focus on power capacity, reliable supply chains, advanced networks, energy efficiency, and AI-driven automation. AI Gigafactories are essential to enhancing Europe's global competitiveness and safeguarding its autonomy in scientific progress and strategic industrial sectors. These infrastructures could foster the development of a European AI processor manufacturing system, thereby reducing the Union's dependence on third countries for the supply of critical technologies. Such a complex infrastructure network requires substantial investment. Accordingly, the European Union is exploring new hybrid investment models that engage both the public and private sectors. At the AI Action Summit held in Paris last February, European Commission President von der Leyen announced the InvestimentAI initiative, a public-private partnership intended to mobilise approximately €200 billion for the development of AI Gigafactories.

European enterprises must be placed in a position to close the gaps in general cloud capacity – typically provided by large-scale data centres – and in edge capacity, which enables similar services to be delivered with significantly lower response times. This is because European data centres have significantly lower

capacity than those in the United States and China, and therefore depend on infrastructures located in non-European countries. Such dependence may negatively impact economic security and public administrations. Through the proposed Cloud and AI Development Act, the Commission aims to encourage investment in cloud and edge capacity to meet European cloud demand by 2035. Given that data centres can adversely affect energy consumption and the environment, the European digitalisation roadmap includes measures designed to ensure that these facilities are energy sustainable.

In order to enhance both the quantity and quality of data for the development of AI models, a new European data strategy will be developed with the aim of creating a single market for cloud services at the European level, targeting both public and private sector users, and designed to be as balanced, secure, and competitive as possible. To provide this infrastructure with a solid regulatory framework, the Commission intends to systematise the fragmented rules applicable to cloud services by developing a Cloud Code that integrates existing codes of conduct and certification schemes on security, energy efficiency, quality, data protection, and data portability. An example is CISPE (Cloud Infrastructure Services Providers in Europe), a European code of conduct for data protection in cloud services. It is compliant with the rules established by the GDPR and was validated by the EDPB in its Opinion 17/2021. In particular, providers adhering to this code are prohibited from using their customers' data for profiling or direct marketing. Common European rules and conditions will also be established for the award of public contracts for data processing services. The Commission will also seek to simplify legislation to reduce administrative burdens and ensure the effectiveness and efficiency of data governance structures. Among the tools to be deployed are Data Labs, which will collect and aggregate data from various AI Factories operating in the same sectors. These infrastructures will not only guarantee access to European data spaces, such as the European Open Science Cloud, but also enhance the interoperability of different data processing and collection systems.

Currently, the application of AI models involves less than 20% of European companies, particularly SMEs. To address this shortcoming, the Commission aims to implement the so-called Apply AI Strategy, promoting innovation and the development of European AI solutions both cross-sectorally and within sectors. This strategy will foster the adoption of AI by the private sector (including strategic industrial sectors such as research, defence, pharmaceuticals, and robotics) and the public sector (services such as health, justice, education, and public administration), with the aim of balancing the protection of fundamental rights with the Union's economic interests.

One of the instruments to support the digitalisation of these sectors will be the European Digital Innovation Hubs, which, in combination with the AI Factories, will enable companies to access computational resources and experimentation spaces through Testing and Experimentation Facilities, particularly in the fields of health, industry and energy, agriculture, and mobility.

Significant investments will also be allocated to Research and Innovation (R&I) through a series of initiatives such as GenAI4EU, under the Horizon 2026–2027 programme, for the development of advanced European AI models, pilot

projects for the digitalisation of public administrations, and the establishment of the European Centre for AI Research, known as RAISE (Resource for AI Science in Europe).

Last March, the Commission launched the Union of Skills strategy[63] with the aim of strengthening the Union's competitiveness through the development and mobility of skills. Its main objectives are: fostering lifelong skills through a solid educational foundation; upskilling and reskilling; promoting skills mobility to unlock the potential of the single market; and attracting and retaining talent from third countries to address skills shortages and nurture top talent within Europe.

In this context, a series of initiatives will be launched to promote digital literacy at all levels of education. These include the 2030 Roadmap for Digital Education, aimed at implementing digital skills among school students and teachers; the establishment of the AI Skill Academy, which will develop curricula focused on new technologies – particularly GenAI – as well as projects to support the reintegration into the workforce of women who have interrupted their careers. To promote skills mobility, measures will be introduced to optimise European legislation that allows highly qualified workers and researchers from third countries to reside in Member States, along with the Marie Skłodowska-Curie Actions MSCA Choose Europe, a European funding programme that supports the training of researchers at both doctoral and postdoctoral level.

The European Union's ambition to become a global benchmark for the development and application of new technologies must be supported by a solid and clear regulatory framework. The proper functioning of the European single market for AI will only be possible if appropriate measures are adopted to implement the AI Act. To this end, the European institutions will promote a series of actions, including the establishment of an AI Act Service Desk within the Office for AI – in collaboration with the network of European Digital Innovation Hubs – to provide practical guidance to AI model providers and deployers (particularly small-scale ones) in achieving regulatory compliance, also offering self-assessment tools; and the creation of the AI Pact, managed by the Office for AI, which encourages and supports European companies in anticipating the adoption of certain provisions of the AI Act. Moreover, public consultations are planned to identify the main shortcomings of the new regulation, along with the establishment of partnerships with third countries in the field of research and innovation.

From what has been examined so far, it is clear that the goal of making the European Union the first 'AI Continent' cannot be achieved without the shared commitment of European and national institutions, researchers, and entrepreneurs.

The significance of the regulatory and normative issues surrounding AI, in relation to the ambivalence of its social implementation as a tool for social inclusion and the anthropocentric promotion of economic development, or for governance and control in what Zuboff calls "surveillance capitalism", pertains

[63] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "The Union of Skills", Brussels, 5.3.2025, COM (2025) 90 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri =CELEX:52025DC0090>.

to a framework of digitization that defines the world and society as an infosphere, augmented by AI. An infosphere that – thanks to Metaverse technologies – makes it possible, within the mass social experiences, to transition from the real (analog) experience to the virtual (digital) one, which now frames life as "Onlife".[64] This mass digital immersion raises concerns about disruptive effects of colonization on social language, where the individual is no longer an empirical individual valued in their singularity (person) at the center of the legal experience[65] but is reduced to a "profile" available for economic and political marketing, governed by algorithms.[66] A condition that could be defined as algocracy, which is fueled by unequal exchanges between "free" services offered to users and their mass datafication for economic and political marketing purposes, and ultimately systemic social control, on the other hand, by an AI imaginary that promises individuals an indefinite expansion of their "creative" experience in the virtual environment provided by the Metaverse(s).

In addition to the clear and concrete economic and social problems (labor market, redefinition of the value chain, access to new digital citizenship), there is the risk of disabling cognitive, operational, and decision-making skills in individuals in favor of greater algorithmic efficiency. This presents a framework where human rights as a whole are at stake. Hence the need for governance of AI technologies and a detailed assessment of the effectiveness of the European regulation on AI in terms of expected outcomes for the protection of fundamental rights related to human dignity, equality, democracy, and the rule of law (Art. 2 TEU).

On the topic of participation in democratic life, De Luca[67] explores the current debate on the relationship between AI and politics, especially after the rise of Generative AI, providing an overview of the challenges and opportunities AI presents in the contemporary political context. The author highlights how AI is altering power dynamics within nation-states and the way these states relate to each other, pointing out an increasing dependence of governments on Big Tech for executive functions such as security and policing. GenAI has also facilitated the emergence of virtual politicians and new forms of political interaction, such as the so-called Augmented Democracy, where digital twins can be used to enhance participation and decision-making processes, thus impacting how political campaigns are conducted.

GenAI has shown a superior persuasive capacity compared to human arguments, making it a powerful tool for influencing public opinion. This raises concerns about public manipulation and the spread of misinformation, due to the non-neutrality of algorithms and techniques like deepfakes. Hence, the need for continuous vigilance from civil society, as well as preventive ad hoc measures. [68] In the AI ecosystem, Big Data, computational power, and automation play a significant role, particularly in how they can impact

[64] Floridi (n 41).
[65] P Grossi, 'Uno storico del diritto in colloquio con Capograssi' (2006) 83(1) Rivista Internazionale di Filosofia del Diritto 13-40.
[66] A Simoncini, 'Il diritto nell'era del dominio tecnico: la lente dell'esperienza giuridica' in G Cazzetta, G Morbidelli and O Roselli (eds.), *Alla ricerca della «dimensione giuridica». Omaggio a Paolo Grossi* (il Mulino 2024) 347-396.
[67] S De Luca, 'Intelligenza Artificiale e politica: l'ultima frontiera' (2024) 3 Storia del pensiero politico.
[68] See also Corasaniti (n 20) 41 ff.

fundamental rights and informational pluralism. The increasing use of generative AI by the media to produce content puts traditional journalistic organizations under pressure, risking market saturation in the information industry, with increased competition from automated systems generating low-cost content.

A key concept addressed is digital constitutionalism, which involves not only the emergence of new rights but also the necessary development of new tools to limit the concentration of power that has shifted from governments to large private digital operators. It is, therefore, necessary to rediscover the dual nature of the concept of constitution, not only as a bill of rights but also as a frame of government. Given that self-regulation by Big Tech is largely illusory,[69] a balance between judicial and legislative power is needed, so that the political-representative circuit can reclaim its role as lawmaker.[70] Additionally, there is the evidence that the impact of AI and digital technologies is not uniform but has asymmetric effects on democracies and authoritarian systems.

In conclusion, in a world increasingly shaped by AI and ICTs, defined in informational terms, a machine may help humans "save the world", but it must never be left alone to decide or choose.[71] It will be crucial, on one hand, to keep in mind the need for constant updates to the regulatory framework in relation to a continually evolving technological reality, and on the other hand, to monitor the effectiveness of the regulatory solutions proposed so far by the AI Act. This implies that it should not be a mere activity of receiving what has been "handed down from above", but rather an ongoing research activity aimed at fully understanding the legal provisions and preparing the necessary technical tools to keep pace with this Revolution.

[69] S De Luca, 'Intelligenza Artificiale e politica: l'ultima frontiera' (2024) 3 Storia del pensiero politico.
[70] O Pollicino, P Dunn, *Intelligenza artificiale e democrazia: opportunità e rischi di disinformazione e discriminazione* (Egea 2024).
[71] Corasaniti (n 20) 43.

Gatt L, Taramelli A, Izzo L, Campanile CC, 'La nuova Legge Quadro per lo Spazio: una innovazione per l'Italia' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252LGATLICCC

EJPLT
ISSN 2704-8012



La nuova Legge Quadro per lo Spazio: una innovazione per l'Italia.

The new Framework Law for Space: an innovation for Italy.

LUCILLA GATT
Full Professor of Private Law, Suor Orsola Benincasa University of Naples
Director, Research Centre of European Private Law (ReCEPL)

ANDREA TARAMELLI
Full Professor of Geograpy
IUSS Pavia

LUIGI IZZO
PhD in Humanities and Technologies: an integrated research path
University of Naples Suor Orsola Benincasa

CARLO CANDELORO CAMPANILE
PhD(s), National PhD Course in Earth Observation
University of Rome "La Sapienza"

Abstract

Questo contributo intende fornire una prima analisi della nuova Legge Quadro italiana per la Space Economy, analizzandone alcuni profili di rilievo e calandola in un contesto caratterizzato sia da una forte competizione internazionale per l'accesso allo spazio sia da nuove tensioni geopolitiche, che rendono imprescindibile lo sviluppo di una filiera nazionale dello Spazio. Emergerà, in particolare, come il Legislatore italiano abbia cercato di rimediare a un ritardo pluridecennale e, ancor più importante, come tale Legge Quadro possieda caratteristiche che potrebbero influenzarne negativamente l'implementazione concreta.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
The present contribution seeks to furnish an initial analysis of the recently instigated Italian Framework Law for the Space Economy. This analysis will examine several of the law's key features and contextualise it within a geopolitical environment characterised by intense international competition for access to space and the emergence of new geopolitical tensions. These developments render the development of a national space industry imperative. In particular, it will become evident how the Italian legislator has sought to remedy decades of delay, and more crucially, how this Framework Law exhibits characteristics that could hinder its practical implementation.

Keywords: Space Economy; Legge italiana per lo spazio; diritto dello Spazio.

Summary: 1. Introduzione: lo sviluppo della Space Economy e la promulgazione della L. n. 89/2025. – 2. L'evoluzione e le prospettive del diritto spaziale internazionale: una breve trattazione. – 3. Il ruolo degli Stati e la "fuga in avanti" di alcuni attori. – 4. La L. n. 89/2025: profili critici. – 4.1. La complessa architettura del procedimento autorizzatorio, tra discrezionalità e articolazione degli uffici. – 4.2. La responsabilità civile dello Stato italiano. – 5. Le prospettive attuative ed economiche della Legge per lo Spazio. – 6. Conclusioni: un'occasione (forse) perduta?

1. Introduzione: lo sviluppo della Space Economy e la promulgazione della L. n. 89/2025.

La Space Economy, attualmente, è oramai un elemento imprescindibile dell'economia tradizionale e "terrestre", in quanto i servizi da essa forniti – Osservazione della Terra, Telecomunicazioni, Navigazione e perfino "cloud orbitali" – sono da un lato integrati nelle attività economiche classiche e nei servizi amministrativi a livello territoriale fungendo da veri e propri "moltiplicatori di forza" e dall'altro sono delle componenti necessarie per assicurare la qualità dei servizi commerciali, dal momento che gli utenti si rivolgono generalmente a quegli operatori che maggiormente – e con profitto – sfruttano le nuove tecnologie, qualunque esse siano.

In particolare, ciò che rileva è la massa dei dati provenienti dai satelliti – SATCOM, GNSS, EO – che costituisce una vera e propria "riserva petrolifera" digitale per una economia ormai sempre più data-driven e che si prevede avrà un valore complessivo di 829 miliardi di euro entro il 2025 nella sola Unione Europea[1]. Anzi, il World Economic Forum, già nell'Aprile 2024 pubblicava un report in cui stimava una crescita talmente repentina per la Space Economy da raggiungere un valore pari a 1800 miliardi di dollari entro il 2035 (vale a dire nell'arco di un decennio)[2].

In più, non manca chi guarda alla Space Economy come ad uno strumento

[1] COMMISSIONE EUROPEA, *European data strategy*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en, che mostra, a titolo di confronto, un valore di circa 301 miliardi di euro nel 2018.
[2] WORLD ECONOMIC FORUM, *Space: The $1.8 Trillion Opportunity for Global Economic Growth – Insight Report*, 2024. Consultabile al sito: https://www3.weforum.org/docs/WEF_Space_2024.pdf

chiave idoneo a innescare una nuova crescita economica[3] e a evitare la trappola della cd. "Secular Stagnation"[4].

E' in tale ottica che andrebbe vista, soprattutto, la recente corsa alle risorse spaziali (minerarie e non) che sta caratterizzando gli ultimi anni e che è uno degli elementi distintivi degli Accordi Artemis promossi dagli Stati Uniti a partire dal 2020, ai quali ha aderito anche il nostro Paese e che hanno di recente visto l'aggiunta del 56mo Paese firmatario[5], il Senegal.

Per cui, è chiaro che lo spazio si è consolidato come leva trasversale di sicurezza, competitività e autonomia strategica tra i vari Paesi con capacità spaziali, catalizzando investimenti, innovazione e capacità industriale. L'Italia pure ha dovuto affrontare la nuova realtà e, se da un lato l'approccio adottato vede la conferma della sua partecipazione alle iniziative sovranazionali (ESA, UE, UNOOSA) e internazionali (Accordi Artemis, collaborazione bilaterale e plurilaterale con altri Paesi anche attraverso iniziative autonome e dedicate[6]), dall'altro persegue ora una maggior autonomia nazionale e un incremento delle capacità industriali e degli investimenti correlati attraverso una rinnovata collaborazione con gli operatori commerciali.

Per conseguire tali obiettivi, il Legislatore ha posto le fondamenta per un framework di riferimento che, almeno per l'Italia, costituisce un passo in avanti di particolare rilievo, ossia la Legge n. 89 del 13 giugno 2025, oggetto di esame in questo contributo. E' degno di nota, poi, che il correlato DDL sia stato proposto nel sessantesimo anno dal lancio del primo satellite italiano - il San Marco - in un ideale trait-d'union tra le origini delle capacità spaziali italiane e i suoi più recenti sviluppi.

Nondimeno è necessario rilevare che l'intervento del Legislatore italiano è – e si vedrà in quale misura – quantomeno tardivo nonché, sotto alcuni profili, caratterizzato da una certa carenza di lungimiranza.

2. L'evoluzione e le prospettive del diritto spaziale internazionale: una breve trattazione.

È necessario considerare che l'azione dei singoli Stati e delle organizzazioni internazionali va calata nel contesto di un framework di norme di diritto internazionale, il cd. Corpus Iuris Spatialis, di cui i principali sono:

- il Trattato sullo spazio extra-atmosferico del 1967 (d'ora in poi Outer Space Treaty);
- l'Accordo sul salvataggio e la restituzione degli astronauti del 1968 (Rescue and Return Agreement);

[3] M. WEINZIERL, *Expanding economic activity in space may offer a solution to secular stagnation*, in *Proceedings of the National Academy of Sciences*, 2023, Vol. 120, 43, e2221347120. https://doi.org/10.1073/pnas.2221347120

[4] S. DI BUCCHIANICO, *A critical analysis of the secular stagnation theory*, Working Paper n° 245, Collana del Dipartimento di Economia dell'Università Roma Tre, 2019. Consultabile al sito: https://economia.uniroma3.it/wp-content/uploads/sites/5/file_locked/2019/10/wp-245.pdf

[5] NASA, pagina ufficiale dedicata agli Accordi Artemis raggiungibile al link https://www.nasa.gov/artemis-accords/

[6] MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE – MAECI, Conferenza sullo Spazio Italia-Africa, Roma, 15–16 luglio 2024, https://www.governo.it/en/node/26225. Consultabile al sito: https://www.youtube.com/watch?v=OaR1mLxJ_kY&t=4s

- la Convenzione sulla responsabilità internazionale per i danni causati da oggetti spaziali del 1972 (Liability Convention);
- la Convenzione sulla registrazione degli oggetti lanciati nello spazio del 1976 (Registration Convention);
- l'Accordo sulla Luna del 1979 (Moon Agreement), che – si noti bene – è quello che ha trovato minore adesione da parte degli Stati, un aspetto che assume rilevanza in considerazione della recente "Corsa alla Luna".

Ad esse su aggiungono anche una serie di strumenti "paranormativi", di origine politica ovvero tecnica (come gli standard CCSDS - Consultative Committee for Space Data Systems e similari), che incidono anche sui profili più strettamente tecnico-procedurali dello spazio.

Il crescente ricorso a strumenti di soft law nel governo delle attività spaziali è dovuto, da un lato, alla difficoltà politica di concludere nuovi trattati multilaterali, dall'altro alla rapidità con cui evolvono le tecnologie e le applicazioni spaziali. Trattasi di approccio che deve confrontarsi con le sfide poste innanzitutto dai divari esistenti tra i Paesi con capacità spaziali avanzate e i Paesi meno avanzati o del tutto privi di tali capacità, giacché i primi possiedono un vantaggio estremamente rilevante ai fini di un potenziale sfruttamento delle risorse spaziali - asteroidi e corpi planetari - e per l'eventuale accesso commerciale allo spazio orbitale e non, oltre che per la relativa militarizzazione.

Ciò comporta la necessità di ripensare l'equilibrio giuridico attuale, in cui l'Outer Space Treaty potrebbe essere correttamente percepito come un elemento normativo anacronistico in relazione a certi suoi elementi[7]. Se di anacronismo si tratti effettivamente, in ogni caso è difficile porvi rimedio con atti di soft law, mancando garanzie certe di equità o sostenibilità. Sicuramente va riconosciuta l'autorevolezza di iniziative come l'IISL – International Institute of Space Law e il The Hague Space Resources Governance Working Group della Leiden Law School, ma non va trascurato come queste iniziative siano prive di quella giustiziabilità che è elemento distintivo degli strumenti di diritto nazionale ed europeo.

Al contempo, il principio secondo cui lo Stato di lancio è internazionalmente responsabile per eventuali danni causati da oggetti spaziali, sancito nella Convenzione sulla responsabilità del 1972, è inadeguato in rapporto alle nuove dinamiche derivanti dalla commercializzazione dello Spazio, specialmente in relazione alla necessità di individuare correttamente lo "Stato di lancio". La responsabilità prevista dalla Convenzione è di tipo oggettivo con riferimento ai danni causati mediante impatto sulla superficie terrestre o con aeromobili in volo. Assume, invece, un carattere di responsabilità per colpa in caso di danni nello spazio extra-atmosferico, richiedendo la prova di negligenza o errore[8]. In più, come dimostra il caso dell'International Space Station Intergovernmental Agreement del 1998 con riferimento alle attività svolte sulla ISS, può anche essere prevista una deroga alla regola generale.

In ultimo, non è presente alcuna norma che disciplini espressamente

[7] N. TANNENWALD, *Law versus Power on the High Frontier: The Case for a Rule-Based Regime for Outer Space*" in *Yale Journal of International Law*, 2004, Vol. 29, 2, 392-394.
[8] M. PEDRAZZI, *Danni causati da attività spaziali e responsabilità internazionale*, Milano, 1996, 234.

l'utilizzo commerciale delle risorse spaziali, siano esse risorse minerarie o altro. Da un lato l'Articolo II dell'Outer Space Treaty statuisce il divieto, per gli Stati, di appropriazione nazionale della Luna e dei corpi spaziali. Dall'altro lato, è difficile applicare estensivamente questa norma agli operatori commerciali. Ipoteticamente, si potrebbe ritenere che, siccome tali operatori agiscono sotto la giurisdizione e responsabilità di Stati, anche ad essi si potrebbe applicare tale divieto di appropriazione. Ciò in quanto gli Stati non potrebbero né disciplinare né consentire una attività che sia stata loro vietata dal medesimo OST. In caso contrario, si giungerebbe a ritenere che gli Stati possano disciplinare e consentire l'appropriazione e circolazione di risorse su cui essi stessi non possono esercitare un controllo di alcun tipo.

Nondimeno in questo vuoto normativo, alcuni Stati – che saranno esaminati brevemente nel prosieguo – hanno adottato legislazioni che riconoscono alle imprese private il diritto di estrarre e appropriarsi di tali risorse, aprendo la strada a una corsa allo spazio ispirata a logiche unilaterali e potenzialmente conflittuali e che vedrebbero le società private agire come "tramite" degli Stati sulla falsariga di quanto fatto con le famose "Società delle Indie" da parte degli Olandesi e Inglesi in pieno colonialismo.

Anzi, gli stessi Accordi Artemis precedentemente menzionati prevedono lo sfruttamento delle risorse spaziali nella *Section 10* dei medesimi (dedicata esclusivamente a tale aspetto), mentre il Memorandum adottato dalla Federazione Russa e dalla Repubblica Popolare Cinese nel 2021 è incentrato sull'esplorazione della Luna mediante una struttura di ricerca stabile ed edificata sul satellite.

Queste iniziative si collocano in un quadro complessivo in cui pure l'International Institute of Space Law ha aperto – nel 2015 – allo sfruttamento delle risorse spaziali con un Position Paper dedicato [9], seguito nel 2019 dall'Hague Space Resources Governance Working Group con un Commentario [10]. Ciò evidenzia non solo la velocità con cui evolvono le prospettive di sviluppo della Space Economy, ma anche la capacità di adattamento degli strumenti internazionali in un contesto in cui i trattati fondamentali costituenti il Corpus Iuris Spatialis rimangono invariati.

3. Il ruolo degli Stati e la "fuga in avanti" di alcuni attori.

Nel contesto del diritto internazionale spaziale, un elemento di rilievo è dato dalla necessaria intermediazione degli Stati ai fini della relativa attuazione[11], essendo privo – come il resto del diritto internazionale – delle caratteristiche di diretta giustizialità proprie del diritto europeo. Sono gli Stati a fornire

[9] IISL BOARD OF DIRECTORS, *Position paper on space resource mining*, 2015. Consultabile al sito: https://iislweb.space/wp-content/uploads/2020/01/SpaceResourceMining.pdf

[10] HAGUE SPACE RESOURCES GOVERNANCE WORKING GROUP, *Building Blocks for the Development of an International Framework on Space Resource Activities*, 2019. Consultabile al sito: https://www.boomportaal.nl/boek/9789462361218#152

[11] R. L. SPENCER JR., *International Space Law: A Basis for National Regulation*, in R. S. JAKHU (a cura di), *National Regulation of Space Activities*, Springer, 2010, 1–16.

concretezza al diritto internazionale mediante atti legislativi interni[12] nonché a innescare nuovi fenomeni mediante la loro opera legislativa – come la liberalizzazione e privatizzazione dello spazio avviata negli anni '80 dagli Stati Uniti – mentre le sedi internazionali forniscono, tutt'al più, delle occasioni di cooperazione tra i medesimi Stati.

Attualmente, circa trenta Paesi hanno adottato legislazioni interne che disciplinano l'autorizzazione e la supervisione delle attività spaziali di enti non governativi.

Sul punto emerge che, da un lato, l'elenco dei Paesi che hanno promulgato legislazioni per la disciplina delle attività spaziali non governative e commerciali è particolarmente esteso e, tralasciando quegli Stati che oggettivamente possiedono e hanno sviluppato indubbie capacità spaziali, comprende anche Paesi oggettivamente piccoli in ogni ambito (finanziario, tecnologico, territoriale e geopolitico) come il Liechtenstein ovvero abbastanza estesi e di non poca importanza economica ma le cui esperienze spaziali non sarebbero ancora al livello di quelle degli Stati più avanzati (si pensi a Cipro, Danimarca, Nigeria, Indonesia, Slovenia).

Dall'altro, solo quattro Stati (Stati Uniti, Lussemburgo, Emirati Arabi Uniti e Giappone), hanno emanato legislazioni ove vengono disciplinati, in termini più o meno dettagliati, anche gli aspetti commerciali relativi all'uso ed allo sfruttamento delle risorse spaziali.

In primo luogo, gli Stati Uniti – che sono gli "artefici" della commercializzazione dello spazio con il "Commercial Space Launch Act" del 1984 e il "Commercial Space Act" del 1995 – hanno promulgato nel novembre 2015 il "Commercial Space Launch Competitiveness Act" che contiene al suo interno delle disposizioni specificamente orientate allo sfruttamento delle risorse spaziali[13], consentendo agli operatori di esercitarvi un diritto di proprietà, peraltro distinguendo tra risorse spaziali in senso lato e risorse provenienti da asteroidi. Ebbene, a fine dicembre 2015 il Board of Directors dell'IISL evidenziò nel suo *Position Paper*[14] due importanti aspetti:

a) La normativa dell'Outer Space Treaty, che ormai ha carattere consuetudinario, impedisce l'esercizio di una sovranità sui corpi spaziali ma è difficile interpretarla anche nel senso che ciò vieti di giungervi, esercitarvi attività estrattive e portar via le risorse accumulate;
b) La normativa del Moon Agreement, al contrario, proibisce espressamente l'appropriazione delle risorse naturali della Luna nella forma di "esercizio di sovranità" e consente solamente l'istituzione di un regime di sfruttamento condiviso e coordinato tra gli Stati (in pratica, una sorta di "diritto d'uso" senza diritti di proprietà sull'area oggetto di sfruttamento), ma non ha natura di diritto consuetudinario, essendo stata ratificata da pochissimi Paesi, tra i quali non figurano – si noti bene – né gli USA, né i maggiori Paesi sviluppati sul piano delle capacità spaziali.

---

[12] G.G. NUCERA, *Recenti sviluppi delle legislazioni spaziali nazionali in ambito europeo*, in S. MARCHISIO e U. MONTUORO (a cura di), *Lo spazio cyber e cosmico – Risorse dual use per il sistema Italia in Europa*, Giappichelli, 2019, pp. 235–242; I. MARBOE, *National Space Law*, in F.G. VON DER DUNK e F. TRONCHETTI (a cura di), *Handbook of Space Law*, Edward Elgar, 2015,130–139.

[13] US CONGRESS, *Space Resource Exploration and Utilization Act of 2015*. Consultabile al sito: https://www.congress.gov/bill/114th-congress/house-bill/1508

[14] *Supra*, nota n. 9

Da ciò consegue che, allo stato attuale, la normativa statunitense non sarebbe affatto in contrasto con le disposizioni di diritto internazionale *effettivamente applicabili nei confronti degli Stati Uniti*, i quali, tra l'altro, sono i promotori dei già citati Accordi Artemis.

Successivamente, sulla scia degli Stati Uniti, altri tre Stati – che non hanno ratificato il Moon Agreement – hanno adottato normative che comprendessero la fattispecie dello Space Mining, ossia (in ordine di tempo):

- Il Lussemburgo nel 2017 ha promulgato la *Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace*[15], che consente agli operatori di agire "uti dominus" nei confronti delle risorse spaziali attribuisce la competenza per il rilascio delle correlate licenze al Ministero dell'Economia, che coordina le attività spaziali nazionali ed esercita i correlati poteri sanzionatori. Ad essa va, però, aggiunta anche la *Loi du 15 décembre 2020 portant sur les activités spatiales*[16], che si pone - rispetto alla legge del 2017 - come "Legge Quadro" per l'intero settore della Space Economy e che ha la particolarità di prevedere espressamente, agli articoli 12 e 13, la possibilità di trasferire la titolarità effettiva delle attività spaziali - la legge utilizza il termine "controllo effettivo" (*actual control*) - dall'originario titolare dell'autorizzazione a un soggetto differente e terzo. Ciò viene contemplato anche nell'ipotesi in cui il terzo acquisti il controllo dell'attività spaziale non mediante l'acquisizione - previa autorizzazione ministeriale - dell'attività stessa ma anche quando assuma una quota di controllo societario nei confronti del soggetto formalmente titolare della concessione;
- Gli Emirati Arabi Uniti già nel 2019 avevano adottato la Federal Law No. (12) of 2019, poi sostituita con il Federal Decree by Law No. (46) of 2023[17] che, all'art. 4, prevede un elenco particolarmente esteso di attività, tra cui anche le attività di sfruttamento delle risorse spaziali, disciplinate all'art. 8 dove si prevedono chiaramente le ipotesi relative a "their acquisition, purchase, sale, trade, transportation, storage and any Space Activities aimed at providing logistical services", in tal modo offrendo una espressione particolarmente ampia del concetto di "sfruttamento delle risorse spaziali";
- Il Giappone, nel 2021, ha approvato il cd. Act on the Promotion of Business Activities for the Exploration and Development of Space Resources[18] che si affianca alla normativa generale adottata nel 2016 e che prevede all'art. 4 un espresso obbligo di trasparenza relativamente alla pubblicazione delle denominazioni dei soggetti titolari delle licenze. Inoltre, utilizza formalmente l'espressione di "space resource mining" e di "space resource extraction", mostrando

[15] LUXEMBOURGH SPACE AGENCY, pagina web con la traduzione in inglese della legge. Consultabile al sito: https://space-agency.public.lu/en/agency/legal-framework/law_space_resources_english_translation.html

[16] LUXEMBOURGH SPACE AGENCY, pagina web con la traduzione in inglese della legge. Consultabile al sito: https://space-agency.public.lu/en/agency/legal-framework/Lawspaceactivities.html

[17] La traduzione ufficiale in inglese è consultabile al sito: https://uaelegislation.gov.ae/en/legislations/2129/download

[18] Una traduzione in inglese è consultabile al sito: https://www.japaneselawtranslation.go.jp/en/laws/view/4332/en

di contemplare chiaramente una condotta tesa attivamente a ottenere queste risorse, andando ben oltre la mera raccolta di esemplari minerari immediatamente accessibili (es. presenti in superficie ovvero appena sotto la superficie del corpo spaziale).

Ebbene, si noti un aspetto, ossia che se due dei Paesi in questione – ossia il Giappone e gli Stati Uniti – sono già in possesso di amplissima esperienza e competenza nell'ambito della Space Economy, lo stesso non può dirsi per gli Emirati Arabi Uniti e per il Lussemburgo, che nondimeno hanno regolamentato non solo le attività spaziali nel complesso ma anche questa specifica ipotesi, ossia lo *space mining*.

Anzi, se è normale prassi fornire incentivi, fiscali non, per incoraggiare la crescita economica di particolari settori, incluso quello della *Space Economy*[19], il Lussemburgo ha adottato un approccio ancor più "aggressivo" in quanto la Legge del 2020 da un lato non prevede un ammontare specifico per l'assicurazione che l'operatore specifico dovrebbe sottoscrivere e dall'altro lato l'art. 16 della medesima estende l'esenzione fiscale dei contratti di assicurazione a quelli che coprono i danni derivanti da attività spaziali. Non solo, come evidenziano alcuni autori [20] la presenza o meno di un contratto di assicurazione non è assolutamente conditio sine qua non per l'ottenimento dell'autorizzazione governativa, ai fini della quale viene considerata adeguata qualsiasi altra forma di garanzia, con la possibilità di impiegare, magari, anche depositi in forma di garanzia. Trattasi di scelta particolarmente vantaggiosa per gli operatori, che potrebbero scegliere di spostare sotto la giurisdizione del Lussemburgo alcune delle attività che conducono.

4. La L. n. 89/2025: profili critici.

Ora, rispetto ai Paesi precedentemente descritti, l'Italia non manca affatto di competenze in ambito spaziale. Nondimeno solo nel 1988 fu istituita formalmente l'Agenzia Spaziale Italiana (ASI), sottoposta nel 1999 [21] alla vigilanza del "Ministro dell'università e della ricerca scientifica e tecnologica". Successivamente, con l'art. 21, d.lgs. 4 giugno 2003, n. 128 (e successive modifiche), sono state poste le basi per un meccanismo che, anche se incentrato sul Ministero dell'Università e della Ricerca, nondimeno assumeva un carattere interministeriale e improntato alla collaborazione tra le amministrazioni potenzialmente coinvolte nelle attività spaziali nazionali, che si è espanso anche attraverso interventi attuati per mezzo di diversi DPCM[22], fino ad assumere una struttura incentrata su più figure, ossia:

- L'Agenzia Spaziale Italiana;

[19] Su questo specifico punto si rinvia a E. I. SCUDERI, *Tax Incentives for the Space Economy and the Potential Impact of Pillar Two*, in *Air and Space Law*, 2024, I, 69-94, dove è possible fruire di una analisi particolarmente estesa e completa delle varie opzioni disponibili.

[20] B. CALMES, L. SCHUMMER e B. GLADYSZ-LEHMANN, *The Space Law Review: Luxembourg*. in J. WHEELER (a cura di) *The Space Law Review*, 2021, 121-131. Consultabile al sito: https://www.arendt.com/wp-content/uploads/2024/04/the_space_law_review_-_edition_4_-_luxembourg.pdf

[21] D.Lgs. 30 gennaio 1999, n. 27

[22] Si vedano il ecreto del Presidente del Consiglio dei Ministri 1° ottobre 2012 e successive modificazioni; il Decreto del Presidente del Consiglio dei Ministri 12 luglio 2022; il Decreto del Presidente del Consiglio dei Ministri 9 febbraio 2023

- Il COMINT (Comitato Interministeriale per le Politiche relative allo Spazio e alla Ricerca Aerospaziale);
- L'autorità delegata in materia spazio dal Presidente del Consiglio dei Ministri (può essere anche un Ministro senza portafoglio);
- Altre Amministrazioni coinvolte tramite il COMINT (es. Ministero della Difesa).

Tali figure sono state preservate nell'articolazione amministrativa prevista dalla L. n. 89/2025, ma ciò comporta una certa confusione. È necessario precisare che la presenza di uffici amministrativi e politici nel settore spaziale, con il compito di delineare i fondamenti della politica da perseguire (al posto dell'Agenzia Spaziale Nazionale), è la norma e, anzi, è una realtà consolidata in tutti gli altri Paesi con capacità spaziali consolidate. Il nocciolo della questione, quindi, riguarda il coordinamento delle attività di questi uffici, con l'obiettivo di accelerarne l'operatività e favorirne le sinergie, evitando che il tutto si riduca in una mera sovrapposizione di competenze.

Prima di procedere oltre e affrontare una prima analisi del nuovo testo legislativo, è necessario operare una premessa.

Infatti, è necessario – sia in fase di stesura sia in fase di assessment applicativo – valutare il testo normativo al fine di evitare rischi di "over regulation" o "under regulation"[23], in quanto la prima ipotesi scoraggia l'iniziativa imprenditoriale mentre la seconda comporta una sostanziale inefficacia dei meccanismi che dovrebbero tutelare gli interessi pubblici in rapporto alle iniziative private. Non solo, sono due fenomeni tra loro strettamente connessi nelle dinamiche[24]. Si tratta, quindi, di comprendere letteralmente come la regolamentazione dovrebbe essere implementata in modo efficiente[25], anche sul piano economico, tant'è vero che si parla del metodo "*Law and Economics*" anche nel contesto italiano[26].

Tuttavia, nessuna delle due ipotesi coincide con quella di una legislazione chiara e ben bilanciata nei suoi elementi costitutivi. Una cosa è verificare se una legislazione sia completa e chiara, altra cosa è discuterne in termini di eccesso o difetto di regolamentazione. Tale distinzione dovrà essere tenuta ben in rilievo nell'esame dei contenuti della Legge Quadro, la quale si intreccia peraltro con l'attività legislativa europea – che ha prodotto recentemente una proposta di Regolamento dedicato a questo settore – e di cui il Legislatore italiano non ha affatto tenuto considerazione nel Dossier di accompagnamento del Disegno di Legge datato 29 ottobre 2024[27], nonostante l'iter di approvazione del DDL sia stato avviato successivamente rispetto all'iniziativa

[23] S. SILEONI e C. STAGNARO, *Prefazione*, in S. SILEONI e C. STAGNARO (a cura di), *Le sfide delle politiche digitali in Europa – Tra iper-regolamentazione e innovazione*, Milano, 2024, 9–10.
[24] Si veda C. R. SUNSTEIN, *Paradoxes of the Regulatory State*, in *University of Chicago Law Review*, 1990, Vol. 57, 2, 413–416, dove – con un paradosso – mette in connessione i due fenomeni.
[25] Sul punto si rinvia a A. SHLEIFER, *Understanding Regulation*, in *European Financial Management*, 2005, Vol. 11, 4, 439–451.
[26] Cfr. G. ALPA, *Il futuro del Law&Economics: le proposte di Guido Calabresi*, in *Contratto e impresa*, 2016, 3, 597-607; G. PASCUZZI, *La definizione del problema nella ricerca interdisciplinare*, in G. BELLANTUONO e U. IZZO (a cura di), *Il rapporto tra diritto economia e altri saperi – La rivincita del diritto*, Napoli, 2022, 55–64; F. PULITINI, *Appunti su la analisi economica del diritto*, in *Quaderni del Dipartimento di Economia dell'Università di Siena*, Working Paper n. 368, 2002; F. CAROCCIA e R. PARDOLESI, *Analisi economica del diritto: 'the Italian Job'*, in *Il Foro Italiano*, 2014, 9, 193–214.
[27] Dossier A.C. 2026 del 29 ottobre 2024. Consultabile al sito: https://documenti.camera.it/leg19/dossier/Pdf/AP0163.pdf

comunitaria, da poco conclusasi con la diffusione di una proposta di Regolamento[28].

Già il fatto che sia stato omesso un riferimento al recente operato della Commissione Europea, all'interno della Relazione di accompagnamento, costituisce un elemento non favorevole, "sanato" solamente con la Relazione aggiornata del 18 marzo 2025[29], peraltro con una breve notazione a pag. 19 che qui si riporta:

"*Da ultimo, come evidenziato in precedenza, si segnala che, nell'ambito del Programma di lavoro della Commissione europea per il 2025 ("Avanti insieme: un'Unione più coraggiosa, più semplice e più rapida", COM(2025) 45) si prevede che nel secondo trimestre del 2025 sarà presentato un atto legislativo sullo spazio volto ad istituire un quadro dell'UE che disciplini la condotta degli operatori spaziali europei.*"

4.1. La complessa architettura del procedimento autorizzatorio, tra discrezionalità e articolazione degli uffici.

Ancor più rilevante è la criticità relativa al procedimento amministrativo delineato all'articolo 7 della L. n. 89/2025, che delinea un procedimento di autorizzazione alquanto complesso e caratterizzato da una struttura doppia, con una prima fase in cui si svolge la verifica del rispetto dei requisiti previsti agli artt. 5 e 6 della medesima Legge, durante la quale l'operatore che chiede l'autorizzazione si interfaccia con l'Agenzia Spaziale Italiana, che cura le attività istruttorie e controlla la sussistenza dei requisiti in capo all'operatore. Ad essa segue, poi e solo in caso di positiva conclusione della prima fase, una ulteriore fase a connotazione fortemente politica e che vede l'intervento di diversi soggetti appartenenti alla sfera più politica della Pubblica Amministrazione, vale a dire i Ministeri e il COMINT (si veda l'art. 2, lett. b), d), e) della Legge).

In più, l'art. 7 prevede che oltre ai Ministeri rappresentati all'interno del COMINT possano essere coinvolte - per ottenerne il parere - anche altre amministrazioni e perfino i servizi di intelligence.

Ebbene, se la prima fase, guidata dall'Agenzia Spaziale Italiana, è caratterizzata da una verifica puntuale e altamente tecnica del rispetto dei requisiti da parte dell'operatore, è palese che la seconda fase vede il potenziale coinvolgimento di numerosi soggetti, alimentando la confusione di una valutazione che presenta, in questo specifico punto, connotati di discrezionalità politica.

Ciò in quanto l'ottavo comma dell'art. 7 delinea tre possibili ipotesi sulla base delle quali, nel corso della seconda fase del procedimento di valutazione istruttoria, è possibile negare l'autorizzazione all'operatore che l'ha richiesta, nonostante il parere positivo dell'Agenzia Spaziale Italiana in ordine al rispetto dei requisiti previsti da questa legge. Il problema è che la formulazione di tali

[28] Alla pagina ufficiale dedicata all'EU Space Act consultabile al sito https://defence-industry-space.ec.europa.eu/eu-space-act_en?prefLang=it è possibile scaricare non solo la *Proposal for a regulation of the European Parliament and of the Council on the safety, resilience and sustainability of space activities in the Union - COM(2025) 335 final* ma anche i relativi allegati e l'analisi di impatto.

[29] Dossier A.S. 1415 del 18 marzo 2025. Consultabile al sito: https://documenti.camera.it/leg19/dossier/Pdf/AP0163b.pdf

cause di esclusione presenti all'art. 7, comma 8, risulta talmente generica da poter consentire una interpretazione giuridica particolarmente ampia e senza che vi sia l'effettivo rischio che gli stessi possano essere ragionevolmente annullati dal giudice amministrativo, una volta impugnati.

Infatti, anche se un diniego di autorizzazione basato su tali ipotesi è difficile da considerare come "atto politico" in senso stretto - che non può essere impugnato davanti al giudice ai sensi dell'art. 7 del decreto legislativo n. 104/2010 - nondimeno può essere qualificato come "atto di alta amministrazione" e quindi essere impugnato, ma il giudice può contestarlo solo se vi sia manifesta illogicità sul piano formale e sostanziale, ossia se sia del tutto irragionevole nei contenuti [30], una eventualità che difficilmente potrebbe accadere in contesti strategici come quello della regolamentazione dello Spazio.

Trattasi di elementi che potrebbero provocare un netto contrasto tra le intenzioni programmatiche del Legislatore e l'effettiva applicazione della Legge medesima, impedendo alle imprese interessate di valutare correttamente la convenienza economica di un investimento in Italia, impattando sull'effettiva competitività del Paese.

Verissimo, nella Relazione allegata all'originaria bozza di legge il Legislatore stesso evidenzia la discrezionalità che connota i procedimenti di rilascio dell'autorizzazione di diversi Paesi, definendolo un controllo

"*di carattere prevalentemente discrezionale ancorché basato su accertamenti aventi sostanzialmente natura tecnica, in ordine alle capacità tecnologiche e finanziarie e in materia di sicurezza e sostenibilità ambientale, in genere demandato alle agenzie spaziali nazionali.*".

Ma, un conto è prevedere un procedimento in cui la decisione finale si fonda anche su criteri discrezionali. Ben altra cosa, invece, è far sì che la decisione finale dipenda soprattutto (se non esclusivamente) da aspetti discrezionali e peraltro formulati in modo assai generico, con la relativa valutazione che viene a dipendere da un numero potenzialmente indefinito di più amministrazioni statali.

Per contro, né il Legislatore francese né quello statunitense – per citare due tra i Paesi più attivi nel comparto – hanno adottato un approccio talmente complesso, preferendo accentrare il tutto in capo a una sola amministrazione e coinvolgendo le altre articolazioni dello Stato solo secondo un criterio di stretta necessità[31].

---

[30] In tema di sindacato del giudice amministrativo sugli atti di alta amministrazione si vedano *ex multis*: Consiglio di Stato, Sez. IV, sent. 27 settembre 2021, n. 6473; Consiglio di Stato, Sez. V, sent. 28 febbraio 2023, n. 2071; Consiglio di Stato, Sez. V, sent. 20 febbraio 2024, n. 1710; Consiglio di Giustizia Amministrativa, Sez. giurisdizionale, sent. 25 marzo 2024, n. 219; Tribunale Amministrativo Regionale per il Lazio, Sez. V bis, sent. 2 aprile 2024, n. 6338; Consiglio di Stato, Sez. III, sent. 4 aprile 2024, n. 3095.

[31] Per la Francia vedasi CENTRE NATIONAL D'ÉTUDES SPATIALES (CNES), *Legislative and regulatory framework – FSOA*, 2024. Consultabile al sito: https://spacecare.cnes.fr/en/la-securite-des-vols-spatiaux-english/legislative-and-regulatory-framework/; per gli Stati Uniti, invece, si faccia riferimento – a titolo di esempio – alla disciplina contenuta nell'US Code of Federal Regulation (US Code of Federal Regulations, Title 15, Subtitle B, Chapter IX, Subchapter D, Part 960, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-IX/subchapter-D/part-960) e che pure è stata considerata come particolarmente complessa dagli

Anzi, il sistema istituito dall'articolo 7 della legge quadro italiana si discosta in modo significativo dagli approcci attuati da due dei suoi principali competitors, gli Stati Uniti e la Francia. Al contrario, sarebbe stato più adeguata l'adozione – per intero – dell'approccio statunitense ovvero francese:

- Seguendo la "via" statunitense, in luogo dell'attribuzione di ulteriori competenze all'ASI con conseguente carico di lavoro eccessivo, potrebbe essere più efficiente istituire un organismo indipendente dall'ASI e incorporarlo in un ministero, secondo una struttura analoga a quella statunitense, ma con giurisdizione su tutti i tipi di satelliti per ragioni di costo. Questo approccio eviterebbe l'adozione dell'architettura statunitense, caratterizzata dalla specializzazione delle agenzie in base al tipo di satellite (ad esempio, la NOAA per i satelliti di osservazione della Terra, la FCC per i satelliti per le telecomunicazioni, ecc.). Tuttavia, è importante notare che la gestione di questo organismo dovrebbe essere condotta in modo da garantire che il suo obiettivo primario rimanga quello di favorire la crescita dell'economia spaziale italiana, circostanza che difficilmente verrebbe perseguita alle condizioni attuali;
- Si potrebbe sostenere, al contrario, che all'ASI dovrebbe essere assegnato un ruolo di guida, come avviene in Francia con il CNES. Tuttavia, va notato che la Francia abbia sempre avuto una politica spaziale organica (fin dagli anni Sessanta), finalizzata non solo alla ricerca scientifica ma anche allo sviluppo del ruolo economico e geopolitico della nazione, dotando il CNES di ingenti risorse.

In entrambi i casi, sia per creare una sorta di "NOAA/FCC/etc omnicomprensiva italiana" sia per rafforzare l'ASI sulla falsariga del sistema francese, si sarebbe dovuto optare per un differimento dell'entrata in vigore della legge.

Probabilmente, l'opzione migliore sarebbe quella di adottare un sistema come quello statunitense, dove la NASA – vale a dire la controparte USA dell'ASI – non ha un ruolo nelle procedure di autorizzazione né può decidere nulla sulla gestione dei servizi a valle, mantenendo il proprio operato incentrato sulla ricerca scientifica. Pertanto, con questo approccio, si dovrebbe creare un ente nuovo e specifico per le attività di licensing, distinto nettamente rispetto all'ASI, con il primo ente che prenderebbe il ruolo del secondo nell'architettura della legge per lo Spazio e con l'ASI che conserverebbe il suo ruolo di ente spaziale nazionale *a vocazione esclusivamente scientifica*.

In realtà, sarebbe corretto dire che l'approccio italiano è un mix tra il modello organizzativo statunitense e quello francese. Questo perché l'articolazione complessiva a livello politico e amministrativo - COMINT, UPSA, eccetera - sembra ricalcare la struttura di alcuni uffici federali del Dipartimento di Stato americano, ma senza la creazione di un organismo ad hoc come NOAA/FCC/eccetera, al posto del quale prevale l'agenzia spaziale nazionale, come nel modello francese.

Oltre a questo, si consideri anche la formulazione della causa di esclusione prevista all'art. 7, co. 8, lett. b), L. 89/2025, talmente ampia da poter

operatori del settore (per accedere ai "Commenti" dei medesimi si veda NOAA, *Comments to the Proposed Rule*, https://www.regulations.gov/document/NOAA-NESDIS-2018-0058-0011/comment).

pregiudicare la partecipazione dell'industria italiana a programmi internazionali, con conseguente "perdita di chance" sul piano economico, industriale, occupazionale e del know-how, atteso che sarebbe impossibile programmare collaborazioni internazionali in un quadro di obiettiva incertezza giuridica[32].

A tale problematica, che riguarda soprattutto le imprese italiane e quelle che desiderino ottenere una autorizzazione senza averne mai avuta una in precedenza, se ne aggiunge un'altra.

Ci si riferisce all'art. 4 della Legge in esame, che oltre a stabilire l'obbligo di ottenere l'autorizzazione, prevede anche due deroghe di rilievo:

- il quarto comma esclude la necessità di ottenere l'autorizzazione se l'operatore sia stato già autorizzato da altro Stato estero con cui sia in vigore un trattato che statuisca il mutuo riconoscimento delle autorizzazioni rilasciate in ottemperanza alla Registration Convention;
- il quinto comma consente di far riconoscere - e, quindi, rendere valida ai sensi della normativa italiana - una autorizzazione rilasciata da uno Stato estero con cui non sia stato stipulato un trattato per il mutuo riconoscimento delle medesime ma che sia stata rilasciata sulla base di criteri di valutazione considerati equivalenti rispetto a quelli impiegati dalle autorità italiane.

Ebbene, attraverso tali deroghe, chi abbia già una autorizzazione rilasciata da un altro Stato è in grado di evitare di dover attivare il procedimento ex art. 7. Ma, se l'art. 28, co. 3 L. 89/2025 prevede espressamente che non si applichi il sistema del silenzio assenso con riferimento al procedimento di autorizzazione ordinario, manca un corrispondente riferimento anche al procedimento di *riconoscimento di autorizzazioni già rilasciate*, e già un autore ha espresso il timore che possa essere attivato il meccanismo del silenzio-assenso[33], in conseguenza del quale, è bene evidenziarlo, delle imprese straniere già operanti nel settore dello spazio potrebbero avere un ingresso "facilitato" nella space economy nazionale, risolvendosi il tutto in una distorsione della concorrenza e in un possibile ostacolo alla crescita di operatori nazionali, con buona pace delle prospettive di sovranità tecnologica che questa legge dovrebbe tutelare.

In verità, questo rischio non dovrebbe sussistere in quanto:

- così ragionando verrebbe meno l'effettivo controllo da parte dello Stato Italiano sulle attività spaziali commerciali, con conseguente inottemperanza delle norme di diritto internazionale;
- si è in presenza di una attività amministrativa connotata da una forte discrezionalità - essendo necessario valutare se i criteri utilizzati dallo Stato estero siano effettivamente equivalenti - e i giudici amministrativi italiani sono tendenzialmente orientati ad escludere che si possa invocare il silenzio-assenso con riferimento alle attività

[32] S. ZOLEA, *La legge italiana sullo spazio nel mondo multipolare*, in S. ZOLEA e T. GRAZIANI (a cura di), *Spazio – Verso una legge italiana*, Callive, 2025, 32–34

[33] F. CASSELLA, *L'autorizzazione amministrativa all'esercizio delle attività spaziali e il ruolo dell'Agenzia Spaziale Italiana*', in S. ZOLEA e T. GRAZIANI (a cura di), *Spazio – Verso una legge italiana*, Callive, 2025, 48.

amministrative ampiamente discrezionali[34];

- l'art. 20, L. 241/1990 chiarisce che questo meccanismo non può applicarsi agli atti e procedimenti che riguardano, tra le varie materie, anche la tutela ambientale, la sicurezza pubblica, la difesa nazionale, la pubblica incolumità, ossia tutti ambiti su cui necessariamente impattano le valutazioni connesse all'opportunità di concedere o meno una autorizzazione a operatori spaziali commerciali.

Nondimeno, però, sarebbe stato opportuno specificare questo aspetto anche in relazione alle procedure di riconoscimento in deroga previste dall'art. 4, esattamente come è stato fatto per il procedimento di autorizzazione "standard" attraverso la previsione dell'art. 28, comma 3, della Legge Quadro.

4.2. La responsabilità civile dello Stato italiano.

Va notato che la struttura del procedimento di riconoscimento in deroga ex art. 4 si pone – in un certo senso – in contrasto con l'art. 10, L. 89/2025, che disciplina il trasferimento della titolarità o del controllo di intere attività spaziali o di singoli oggetti spaziali, una pratica particolarmente rilevante nel contesto della *Space Economy*[35]. Ciò in quanto entrambe le fattispecie comportano la possibilità che lo Stato italiano si trovi ad essere responsabile ai sensi della Liability Convention.

Ma, se l'art. 10 prevede che si segua la procedura delineata all'art. 7, con tutti i controlli e meccanismi prudenziali ad esso connessi in modo da evitare pratiche elusive[36] degli obblighi risarcitori previsti dalla Liability Convention e fenomeni ben più pericolosi come il "mercato nero" dei satelliti[37], nondimeno tale attenzione pare essere assente nel procedimento di riconoscimento delle autorizzazioni estere, essendo caratterizzato da una struttura notevolmente più snella e semplice e con la valutazione incentrata solamente sull'autorità ministeriale delegata allo Spazio.

Eppure, nel momento in cui si riconosce la validità dell'autorizzazione già rilasciata, lo Stato Italiano dovrebbe assumere responsabilità giuridico-economiche – descritte agli artt. 18-21 L. 89/2025 in tema di responsabilità civile per danni da operazioni spaziali – pari a quelle derivanti dal rilascio *ex novo* di autorizzazioni.

Ciò posto, si esamina ora l'architettura di tale sistema di responsabilità civile, una problematica che incide pesantemente su profili economici e in relazione

---

[34] Sul punto vedasi Consiglio di Stato, Sezione IV, sent. 5 settembre 2016, n. 3805.

[35] A. VETTOREL, *La compravendita transnazionale dei satelliti artificiali in orbita nella New Space Economy,* in *Diritto del commercio internazionale*, 2024, 2, 499-516; F. G. VON DER DUNK, *Transfer of Ownership in Orbit: from Fiction to Problem*, in M. HOFMANN e A. LOUKAKIS (a cura di) *Ownership of Satellites: 4th Luxembourg Workshop on Space and Satellite Communication Law*, Nomos Verlagsgesellschaft and Hart Publishing, 2017, 29–43; R. S. JAKHU, B. JASANI e J. C. MCDOWELL, *Critical issues related to registration of space objects and transparency of space activities*, in *Acta Astronautica*, 2018, Vol. 143, 406-420; U. DASGUPTA, *On-Orbit Transfer of Satellites between States*, in *International Institute of Space Law*, 2016, 7, 641-666; A. KERREST, *Legal Aspects of Transfer of Ownership and Transfer of Activities*, in *International Institute of Space Law*, 2012, 10, 794-800.

[36] T. LIAMETI, P. BROUMA AND D. ANAGNOSTOPOULOU, *Transfer of Ownership In-Orbit: Shaking the Status Quo and Recalibrating the Registration and Liability Regimes*, in *International Institute of Space Law*, 2021, 1, 3-14; A. VETTOREL, *La nuova disciplina della responsabilità dello Stato e dei privati per le attività spaziali*, in S. ZOLEA e T. GRAZIANI (a cura di), *Spazio – Verso una legge italiana*, Callive, 2025, 203-206.

[37] G. A. LONG, *Black Market Launches of Small Satellites*, in *International Institute of Space Law*, 2016, 4, 401-417.

alla quale è necessario individuare un bilanciamento tra le aspettative degli operatori e le necessità economiche e finanziarie dello Stato.

L'articolo 18, che sembra riferirsi specificatamente alla responsabilità civile a livello nazionale (ovvero al caso in cui un operatore satellitare italiano danneggi un altro soggetto italiano o un operatore satellitare italiano), stabilisce nel primo comma la responsabilità oggettiva e omnicomprensiva dell'operatore spaziale, introducendo poi una ulteriore specificazione relativa ai casi di impatto con la superficie terrestre e con aeromobili in volo che causano danni a persone o cose a bordo (art. 18, co. 2). Questa particolare formulazione sembra non ricomprendere i danni derivanti da collisioni tra oggetti spaziali appartenenti a soggetti differenti.

È difficile capire se i due commi dell'art. 18 debbano essere interpretati nel senso che il secondo stabilisce semplicemente una presunzione di responsabilità da parte dell'operatore satellitare in relazione a specifiche ipotesi di danno. L'alternativa sarebbe quella di considerare il primo comma come una disposizione di principio, mentre il secondo comma costituirebbe una limitazione della responsabilità dell'operatore con riferimento a casi specifici.

Sembra essere la prima opzione, poiché è evidente che il legislatore ha modellato il regime di responsabilità civile secondo il modello di responsabilità per l'esercizio di attività pericolose delineato all'art. 2050 c.c. Ciò è dimostrato dal fatto che l'art. 18 di questa nuova legislazione impone all'operatore l'onere di provare la responsabilità esclusiva di un terzo che abbia causato intenzionalmente il danno o che il danno sia stato causato esclusivamente dal comportamento della parte lesa.

Al contrario, nel caso di un contributo causale da parte del danneggiato, si applica l'art. 1227 c.c., con tutte le conseguenze in termini di riduzione dell'entità del risarcimento

Adottando questo ragionamento, l'ipotesi di "incidenti" orbitali rientrerebbe nell'ambito della normale responsabilità per danni, senza alcuna presunzione di responsabilità e con l'applicazione delle normali regole di prova nei procedimenti giudiziari. Questa sembra, infatti, essere l'unica opzione possibile. Infatti, se il successivo art. 19 della legge richiama l'intera Liability Convention, compresa la fattispecie delle collisioni in orbita, al fine di ottemperare agli obblighi internazionali, ne consegue che l'articolo 19 tutela certamente le parti straniere che subiscono un danno a causa di un evento di questo tipo. Interpretare l'articolo 18 in modo diverso da quanto suggerito nelle righe precedenti, ovvero in modo tale da escludere, a livello nazionale, la responsabilità per i danni causati da "collisioni orbitali", comporterebbe una disparità di trattamento per i cittadini italiani danneggiati nel corso di una collisione in orbita.

Tuttavia, proprio la formulazione di questo punto dell'art. 18 induce a perplessità circa la mancata menzione di una ipotesi di responsabilità identica a quella contemplata nell'art. III della Liability Convention. Infatti, un terzo estraneo all'operazione spaziale potrebbe causare danni innescando il rientro incontrollato di un satellite - magari con un cyberattacco - ma potrebbe provocarli anche conducendo l'oggetto spaziale a schiantarsi in orbita contro un altro oggetto spaziale. Se si guarda, invece, dal punto di vista del danneggiato, non si comprende come un danneggiato possa "concorrere a

provocare il danno" nell'ipotesi di impatto con la superficie terrestre, a meno che non sposti beni di sua proprietà in prossimità del punto di ipotetico impatto dell'oggetto spaziale. Ben più plausibile, invece, diventa l'ipotesi del concorso causale (o dell'esclusiva responsabilità) del danneggiato se si pensa a una manovra errata di un satellite operata dal danneggiato stesso e attuata in orbite particolarmente affollate.

Di nuovo, così ragionando emerge netta la paradossale assenza di un sistema analogo all'art. III della Liability Convention anche per i casi di danneggiamento che rientrino interamente nella giurisdizione nazionale (ossia in cui sia il danneggiante sia il danneggiato abbiano nazionalità italiana).

Detto questo, in ogni caso l'operatore è normalmente chiamato a rispondere del danno nei limiti del massimale assicurativo previsto dall'art. 21, commi 21 e 2, che ha una soglia massima pari a 100 milioni di euro e una soglia minima pari, a seconda della fattispecie, a 50 o 20 milioni di euro, secondo un meccanismo di graduazione che dovrà essere ancora definito e che sicuramente sarà attuato in modo da ridurre l'esposizione economica dello Stato conseguente all'attuazione della legge, tant'è vero che in più punti dei lavori preparatori pubblicati insieme al testo definitivo della Legge Quadro nonché al quarto comma dell'art. 24 è chiarito che dall'attuazione della medesima non devono derivare - in relazione a specifiche attività di alcuni enti, come Ministeri e COMINT - nuovi o maggiori oneri per la finanza pubblica.

In ragione di ciò, il risultato che emerge dalla lettura congiunta degli articoli 18, 19, 20 e 21 della Legge Quadro è il seguente:

a) Nel caso in cui un soggetto italiano sia danneggiato da un operatore operante da un altro Stato, il danneggiato può presentare istanza di risarcimento in via diplomatica ai sensi dell'art. 20 delle Legge Quadro (che rimanda ai meccanismi della Liability Convention) e ottenere sempre e comunque un risarcimento integrale, anche se dovesse pagare lo Stato Italiano in luogo dello Stato estero;
b) Nel caso in cui un soggetto straniero venga danneggiato da un operatore autorizzato dallo Stato Italiano e riceva integrale risarcimento, lo Stato Italiano può poi rivalersi nei confronti dell'operatore responsabile entro i limiti del massimale dell'assicurazione, con la conseguenza che non recupera interamente quanto risarcito allo Stato estero;
c) Nel caso in cui un soggetto italiano sia danneggiato da un operatore autorizzato dallo Stato italiano, dovrà agire direttamente contro l'assicuratore dell'operatore in questione e sarà risarcito entro il limite del massimale, senza poter contare sulla garanzia dello Stato italiano per la parte di danno eccedente il massimale assicurativo.

Per cui, si prospetta una situazione particolare, in cui un soggetto italiano che abbia subito un danno da un oggetto spaziale deve sperare che il medesimo sia di proprietà di un operatore estero non autorizzato in Italia, altrimenti potrebbe non essere integralmente risarcito. Trattasi di situazione che, da un lato contribuisce a contenere i costi per le casse dello Stato italiano e, dall'altro, potrebbe sollevare dubbi in ordine alla sua ragionevolezza[38]. Non solo, se si

[38] I. CASTELLUCCI, *Il d.d.l. "Spazio" 2024: danno, responsabilità, questioni assicurative*, in S. ZOLEA e T. GRAZIANI (a cura di), *Spazio – Verso una legge italiana*, Callive, 2025, 64-68.

guarda appunto al profilo del "danno economico" per lo Stato conseguente al pagamento, da parte sua, del risarcimento versato per danni provocati da operatori da esso autorizzati ai sensi dell'art. 19 della Legge Quadro, anche il diritto di rivalsa dello Stato è limitato dal massimale di 100 milioni di euro.

Quindi, può ben verificarsi l'ipotesi in cui lo Stato debba risarcire un soggetto estero ai sensi dell'art. 19 per un valore superiore ai 100 milioni di euro e senza poter incamerare l'intera somma corrispondente mediante il meccanismo di rivalsa nei confronti dell'operatore effettivamente responsabile.

5. Le prospettive attuative ed economiche della Legge per lo Spazio.

Sul piano prettamente attuativo, valga innanzitutto una semplice considerazione, ossia che la L. 89/2025 è entrata in vigore immediatamente, senza un periodo transitorio, in contrasto con quanto deciso dal Legislatore transalpino, che ha predisposto un periodo transitorio di due anni.

Tale aspetto avrebbe avuto un rilievo positivo sotto due elementi:

a) Con riferimento all'adeguamento degli organici dell'Agenzia Spaziale Italiana che, ai sensi degli artt. 7, 11, 12, 13 e 14 L. 89/2025, assume un ruolo di rilievo come autorità di vigilanza ma disponendo di un organico particolarmente risicato e destinato ad essere aumentato, dal momento che al 31 dicembre 2023 risultavano poco più di 400 dipendenti a tempo indeterminato nell'organico dell'Agenzia Spaziale Italiana[39] unitamente a una manciata di stagisti e ricercatori a tempo determinato e che gli eventuali incrementi alla data del 31 dicembre 2024, resi noti presumibilmente nei prossimi mesi, saranno sicuramente risibili rispetto alle esigenze derivanti dai compiti attribuiti all'ASI;
b) Con riferimento all'attuazione della L. 89/2025 per mezzo dei decreti attuativi "a valle", previsti dall'art. 13 L. 89/2025 e per la cui adozione è previsto che il Presidente del Consiglio adotti questi decreti – almeno 5 tra DM e DPCM, oltre alla modifica dei regolamenti esistenti – di concerto con sette Ministeri differenti, dopo aver acquisito il parere del Consiglio di Stato e a seguito dell'audizione di almeno altre 3 differenti amministrazioni, tra cui l'ASI.

Nondimeno, il Legislatore ha optato per una immediata entrata in vigore che, tuttavia, è solo apparente, mancando sia le norme regolamentari di attuazione sia le risorse – in termini di personale – necessarie per l'ASI.

Sotto il profilo economico, invece, si rileva la presenza – agli artt. 22 ss. – di norme apparentemente in linea con gli obiettivi di rilancio della *Space Economy*, per cui l'unico nodo reale sembra sia relativo alle risorse effettivamente disponibili.

Infatti, l'art. 22 prevede che venga redatto un "Piano nazionale per l'economia dello spazio ", uno strumento di programmazione su un periodo non inferiore ai 5 anni e di cui si deve provvedere all'aggiornamento su base biennale, avente l'obiettivo di mettere a sistema le capacità di ricerca universitarie e aziendali nonché di ottimizzare l'impiego delle risorse pubbliche,

[39] AGENZIA SPAZIALE ITALIANA, *Modello 2023 IR 8565 1 ERIC - Conto e costo del personale*. Consultabile al sito: https://asi.portaleamministrazionetrasparente.it/archiviofile/asi/04-%20Personale/Conto%20e%20costo%20del%20personale/modello_2023_IR_8565_1_ERIC_signed.pdf

anche attraverso il ricorso al Partenariato Pubblico-Privato. Pertanto, una parte degli effetti economici dovrebbe essere di natura "indiretta", dovuta in primis al ricorso al Partenariato Pubblico Privato, finanziato mediante appunto il fondo istituito all'art. 23, nonché con l'attuazione del principio dell'accesso equo alle infrastrutture e ai dati spaziali e con il coinvolgimento delle Piccole e Medie Imprese (PMI) in termini di accesso delle medesime imprese agli appalti in materia spaziale, prevedendo agli art. 24 e 27 un sostanziale raccordo con il Codice dei Contratti Pubblici (Decreto Legislativo n. 36/2023) e un maggior ricorso al subappalto, in parte obbligatorio e in parte "premiale", al fine di far sì che negli appalti in ambito spaziale una quota del valore dei medesimi venga assegnata a start-up innovative e a Piccole e Medie Imprese.

Tuttavia, le risorse specificamente allocate per l'anno 2025 nel fondo dedicato sono particolarmente irrisorie e ammontano a soli 35 milioni di euro.

6. Conclusioni: un'occasione (forse) perduta?

Sicuramente questa Legge costituisce un rilevante passo in avanti in quanto consente di supportare attivamente la *Space Economy* nazionale, anche da un punto di vista giuridico. Se a ciò si aggiunge la progressiva obsolescenza dell'ordinamento internazionale in materia di Diritto Spaziale, diviene ancor più rilevante il ruolo delle legislazioni nazionali per disciplinare un comparto in rapidissima crescita.

Però, è necessario effettuare un paio di notazioni conclusive.

In primo luogo, nell'ambito della legislazione italiana un ruolo di rilievo è assegnato all'ASI, istituita in tempi "recenti" e con una *mission* incentrata sulla ricerca scientifica.

Ad essa, ora, si affiancherebbe – oltre ai compiti descritti prima in tema di autorizzazione amministrativa – anche un ruolo di "propulsore" della crescita delle PMI che caratterizzano il tessuto economico e industriale italiano.

Ma, in verità, riesce difficile immaginare che l'ASI possa svolgere questo particolarissimo compito, a meno che non venga operato un cambio di rotta particolarmente drastico.

Per meglio considerare questa perplessità e supponendo che si voglia sempre seguire il modello francese, è necessario considerare una differenza rilevante tra ASI e CNES, dal momento che il legislatore italiano sembra aver adottato, sotto alcuni aspetti, una struttura simile a quella francese.

Il CNES è stato istituito nel 1961 con la Loi n. 61-1382, nel contesto di un'intensa competizione tra USA e URSS e per volontà del Presidente De Gaulle, sostenitore dell'indipendenza tecnologica, geopolitica, militare e nucleare della Francia[40]. Di conseguenza, il suo approccio trascende gli ambiti della ricerca scientifica convenzionale e della semplice fornitura di supporto alle politiche spaziali. Infatti, ha stretti legami sia con le forze armate (il primo direttore generale era un ufficiale militare e l'attuale struttura di governance comprende un generale con una vasta esperienza) sia con le aziende del settore aerospaziale.

[40] J. PENEZ, *L'essor de la politique spatiale française (1959-1964)*, in *Vingtieme siecle. Revue d'histoire*, 1996, 50, 132-136.

Al contrario, l'ASI è stata fondata solamente quasi trent'anni dopo, nel 1988, e ha svolto un ruolo prevalentemente scientifico (si consideri che per lungo tempo è stata sotto il controllo esclusivo del Ministro dell'Università e della Ricerca), acquisendo solo di recente la responsabilità di operare un collegamento tra lo Stato e le aziende del settore. Tuttavia, non possiede né la struttura né la "mentalità" previste da De Gaulle per il CNES (anzi, a proposito di militari, l'ufficiale più alto in grado nell'organigramma dell'ASI è un tenente colonnello con ampie qualifiche accademiche). Quindi, anche cercando di adottare il modello organizzativo "europeo" (dove i servizi a monte e quelli a valle sono gestiti dalla stessa entità), è difficile pensare che l'ASI, che non è paragonabile al CNES francese, possa gestire adeguatamente tutte queste responsabilità.

Di conseguenza, sarebbe più vantaggioso dal punto di vista finanziario, in una prospettiva a lungo termine, adottare un modello organizzativo simile a quello utilizzato dagli Stati Uniti.

Anzi, per meglio specificare ancora, si consideri che negli USA non solo la gestione, la supervisione e l'autorizzazione delle attività economiche nel settore spaziale sono condotte senza il coinvolgimento dell'agenzia spaziale nazionale e creando uno o più organismi pubblici specificamente responsabili di questo scopo, ma si attinge anche all'esperienza consolidata dell'autorità nazionale per la sicurezza del volo (che per noi sarebbe l'ENAC).

Sarebbe una scelta anche in linea con la pregressa esperienza maturata dall'ENAC stessa già coinvolta nella regolamentazione delle attività suborbitali – che, paradossalmente, la nuova legge italiana ricomprenderebbe nella nozione di attività spaziali [41] – e si sarebbe potuto considerare questo coinvolgimento nella concessione di licenze per le attività orbitali come una naturale "estensione" del suo attuale mandato[42], proprio come avviene negli Stati Uniti con la FAA.

Questo approccio consentirebbe all'ASI di mantenere le sue caratteristiche statutarie, consentendo al contempo al nuovo organismo di concentrarsi esclusivamente sul potenziamento dell'economia spaziale nazionale, obiettivo

---

[41] Infatti, si consideri la formulazione dell'art. 2, lett. a) della legge in esame, che statuisce come segue: "*«attività spaziale»: il lancio, il rilascio, la gestione in orbita e il rientro di oggetti spaziali, compresi lo smaltimento dalle orbite terrestri e la rimozione di oggetti, i servizi in orbita, l'assemblaggio e l'utilizzo di stazioni spaziali orbitanti nonché la produzione di oggetti nello spazio extra-atmosferico e sui corpi celesti; l'esplorazione, l'estrazione e l'uso delle risorse naturali dello spazio extra-atmosferico e dei corpi celesti, in conformità agli strumenti giuridici adottati a livello internazionale; il lancio, il volo e la permanenza, di breve o di lungo periodo, di esseri viventi nello spazio extra-atmosferico e sui corpi celesti; le attività condotte attraverso le piattaforme stratosferiche e i razzi sonda; ogni altra attività realizzata nello spazio extra-atmosferico e sui corpi celesti da operatori cui si applica la presente legge;*". Ora, questa scelta non sarebbe precisamente appropriata, poiché la stratosfera è una parte dell'atmosfera terrestre corrispondente ad altitudini comprese tra 10.000 e 60.000 metri, ovvero ben 40.000 metri al di sotto della linea di Karman, un confine convenzionale che separa l'atmosfera terrestre dallo spazio vero e proprio, adottato anche dalle principali agenzie nazionali per la sicurezza aerea, come la FAA statunitense, che ha adottato l'altitudine di 80km come soglia per poter qualificare un soggetto come "commercial astronaut" (https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8800.2.pdf). La stessa Aeronautica Militare Italiana considera suborbitali le attività condotte al di sotto di un'altitudine di 100 km (https://www.aeronautica.difesa.it/home/noi-siamo-l-am/spazio-e-aerospazio/). Ma a questo punto, perché un simile approccio totalmente opposto rispetto ai maggiori competitor stranieri?

[42] ENAC, *Audizione Presidente Enac Avv. Pierluigi Di Palma*, 03 dicembre 2024 (X commissione della Camera dei Deputati). Consultabile al sito: https://documenti.camera.it/leg19/documentiAcquisiti/COM10/Audizioni/leg19.com10.Audizioni.Memoria.PUBBLICO.ideGes.51923.02-12-2024-13-46-39.247.pdf

da raggiungere senza influenze provenienti dal carattere puramente "scientifico" dell'ASI, e consentirebbe inoltre di capitalizzare l'esperienza già acquisita dall'ENAC e dall'Aeronautica Militare Italiana. Questo approccio è stato seguito anche dal legislatore britannico; infatti, la Civil Aviation Authority (CAA) del Regno Unito agisce come autorità di settore in collaborazione con l'Agenzia Spaziale Britannica. Questa struttura è simile a quella degli Stati Uniti, ma si basa sulla diversa esigenza di garantire l'imparzialità nel processo di autorizzazione, alla luce della considerazione che l'Agenzia spaziale britannica era inizialmente incaricata sia di rilasciare licenze per le attività spaziali sia di promuovere attività nell'ambito dell'economia spaziale, sollevando dubbi sull'effettiva imparzialità dell'Agenzia spaziale[43]; allo stesso tempo, la CAA britannica è considerata più adatta a svolgere le funzioni in questione, data la sua esperienza come autorità di regolamentazione. La medesima scelta è stata fatta anche dal Canada e dalla Norvegia.

La seconda e ultima notazione conclusiva, invece, attiene a un elemento che ulteriormente distingue - ancora non si può dire se in negativo o positivo anche se si ha la sensazione che sia un elemento pesantemente negativo - la Legge Quadro italiana da quelle dei principali *competitors*. Infatti, a differenza di alcuni Paesi, nello specifico gli USA, il Lussemburgo e gli UAE di cui è stata anche fatta una articolata comparazione da parte di VON DER DUNK[44], manca una disciplina sullo sfruttamento commerciale delle risorse minerarie spaziali, inclusa solo in forma di principio nel contenuto dell'art. 2 della Legge Quadro e per niente affrontata altrove.

Tale mancanza di una disciplina approfondita, in un periodo storico in cui il relativo dibattito è particolarmente acceso[45] e diversi Stati hanno già legiferato prevedendo framework specificamente rivolti in tale direzione, comporta un rischio di irrilevanza dell'Italia come Paese, una volta che si dovrà necessariamente rinegoziare i contenuti del diritto internazionale dello Spazio. Al contempo, si pone concettualmente in contrasto con l'adesione agli Accordi Artemis, che prevedono anche attività di sfruttamento delle risorse spaziali.

In più, fornisce ai potenziali operatori italiani minori opportunità per entrare nella *Space Economy*. Ciò in quanto l'art. 3 prevede che la Legge Quadro si applichi anche alle attività spaziali svolte da operatori italiani al di fuori del territorio italiano. Ma come si pone la situazione se un operatore italiano, partendo da un altro Paese che disciplina questa fattispecie, si propone di entrare nel settore dello *Space Mining*? Quali condizioni sarà necessario rispettare per ottenere l'autorizzazione da parte delle autorità italiane?

---

[43] UK GOVERNMENT, *Explanatory memorandum to the space industry regulations 2021 - Draft Statutory Instrument No. 792*, 5 e ss.. Consultabile al sito: https://www.legislation.gov.uk/uksi/2021/792/memorandum/contents

[44] F.G. VON DER DUNK, *Property Rights Over the Moon or On the Moon? The Legality of Space Resource Exploitation on Celestial Bodies*, in *Journal of Law & Innovation*, 2023, 1, 96-134.

[45] E. TEPPER, *Structuring the Discourse on the Exploitation of Space Resources: Between Economic and Legal Commons*, in *Space Policy*, 2019, Vol. 49, 101290, https://doi.org/10.1016/j.spacepol.2018.06.004; J. SU, *Legality of unilateral exploitation of space resources under international law*, in *International and Comparative Law Quarterly*, 2017, 4, 991-1008, doi:10.1017/S0020589317000367; F.G. VON DER DUNK, *Asteroid Mining: International and National Legal Aspects,* in *International Law Review*, 2017, 1, 83-102; F. TRONCHETTI, *Legal aspects of space resource utilization*, in F.G. VON DER DUNK e F. TRONCHETTI, *Handboook of Space Law*, Elgar, 2015, 769-813.

Nel dubbio, potrebbe risultare ben più conveniente costituire una nuova impresa nel territorio dello Stato prescelto per l'avvio di attività di Space Mining, in quanto avrebbe formalmente la nazionalità di quello Stato e non necessiterebbe di una autorizzazione da parte anche dello Stato italiano. Ciò significa, però, che in relazione a tali attività spaziali, gli Stati dotati di una legislazione articolata si trovano nelle condizioni di attirare imprese e capitali, forti di una oggettiva certezza del diritto, quantomeno a livello nazionale, costituendo così una occasione perduta per il Legislatore italiano.

Gavriil E, Pavlidis G, 'The fog of information: the EU AI Act and legal strategies against AI-fuelled disinformation' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252EGGP

EJPLT
ISSN 2704-8012



The fog of information: the EU AI Act and legal strategies against AI-fuelled disinformation

La nebbia dell'informazione: l'AI Act dell'UE e le strategie giuridiche contro la disinformazione alimentata dall'IA

ELENI GAVRIIL
Lecturer in International Economic Law and Human Rights
Neapolis University Pafos

GEORGIOS PAVLIDIS
Associate Professor of International and EU Law, UNESCO Chair
Neapolis University Pafos

Abstract

The rise of generative AI has complicated longstanding challenges in the fight against disinformation, enabling the creation and spread of synthetic content at unprecedented speed and scale. While disinformation is not new, AI's ability to impersonate credible sources, manipulate audiovisual material, and craft persuasive narratives across languages raises urgent legal and regulatory concerns. This article examines the provisions of the EU Artificial Intelligence Act (AI Act), which can provide innovative responses to AI-driven disinformation. The AI Act does not address disinformation in a direct manner, but it establishes mechanisms that are relevant to this emerging problem. The article situates the AI Act within the broade EU regulatory landscape, which also includes the Digital Services Act, the Code of Practice on Disinformation, and the EU Charter of Fundamental Rights. The focus is on the risk-based classification and transparency rules of the AI Act, which can enhance democratic resilience, if they are paired with the necessary safeguards.

This study was prepared in the context of the Jean Monnet Centre of Excellence AI-2-TRACE-CRIME (Project 101175740) and was funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
L'ascesa dell'intelligenza artificiale generativa ha complicato sfide già note nella lotta contro la disinformazione, rendendo possibile la creazione e la diffusione di contenuti sintetici con una velocità e una portata senza precedenti. Sebbene la disinformazione non sia un fenomeno nuovo, la capacità dell'IA di imitare fonti credibili, manipolare contenuti audiovisivi e costruire narrazioni persuasive in più lingue pone interrogativi giuridici e regolatori urgenti. Questo articolo analizza il Regolamento europeo sull'intelligenza artificiale (AI Act), che rappresenta una risposta innovativa, sebbene indiretta, alla disinformazione generata dall'IA. Pur senza affrontare esplicitamente il fenomeno, l'AI Act introduce strumenti rilevanti per i nuovi disordini informativi. L'analisi colloca il Regolamento nel più ampio panorama normativo dell'UE, che comprende il Digital Services Act, il Codice di buone pratiche sulla disinformazione e la Carta dei diritti fondamentali dell'Unione europea. L'attenzione è posta sul sistema di classificazione basato sul rischio e sulle norme di trasparenza previste dall'AI Act, che possono rafforzare la resilienza democratica se accompagnate dalle necessarie garanzie.

Keywords: AI Act; disinformation; generative AI; synthetic content; EU law; risk-based regulation; transparency obligations; freedom of expression; digital governance; platform accountability

Summary: 1. Introduction – 2. Disinformation meets AI: Definitions and Regulatory Tensions. – 3. Regulatory Tools in the EU AI Act for Combating AI-Driven Disinformation. – 4. Legal Strategies Against AI-Fuelled Disinformation. – 5. Critical Assessment and Future Directions.

1. Introduction.

Our time has been described as a post-truth era,[1] in which public opinion seems to be guided more by emotions and personal beliefs than by objective facts.[2] For the purposes of this article, the term 'disinformation' is defined as the intentional spread of false or misleading information, which has become a serious threat to modern democracies. The problem seems to have been magnified by the rise and viral nature of digital platforms, as well as the emergence of large language models (LLMs), deepfakes, and other generative AI technologies. What used to require manual effort can now be automated and scaled up. Disinformation can also be tailored to individuals and situations with great speed and reach. For example, in the run-up to Slovakia's 2024 parliamentary elections, AI-generated audio recordings were circulated to impersonate a candidate, containing fake statements.[3] In the United States, during the 2024 primary season, there have been deepfake videos using President Biden's voice, urging US citizens not to vote. This illustrates how

[1] S Lewandowsky, U KH Ecker and J Cook, 'Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era' (2017) 6 Journal of Applied Research in Memory and Cognition 353.
[2] C Galletta Horner and others, 'Emotions: The Unexplored Fuel of Fake News on Social Media', *Fake News on the Internet* (Routledge 2023) 1039-1066.
[3] M Meaker, 'Slovakia's Election Deepfakes Show AI Is a Danger to Democracy' (*Wired*, 10 March 2023) <https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/> accessed 11 July 2025.

generative AI can be misused to undermine public trust and electoral processes in modern democracies.[4] A similar pattern has been observed in Singapore, where the announcement of the 2025 general elections was followed by a spike in AI-generated political content online, as part of attempts to affect voters' ability to make informed decisions.[5]

A complex regulatory challenge emerges, as AI is integrated into the information ecosystem. Could legal frameworks keep pace with the tactics of those who exploit AI to distort public discourse, without compromising freedom of expression and opinion? Prompt-driven propaganda, lifelike synthetic avatars, and deceptively real fake videos are part of today's reality, they are no longer speculative. Not surprisingly, there are widespread concerns and calls for regulatory action. Against this backdrop, the article examines how the European Union is responding to the threat of AI-powered disinformation, with an emphasis on the Artificial Intelligence Act (AI Act). It assesses the role of the AI Act within the EU's wider digital governance agenda and considers how it might strengthen the regulatory response to algorithmically amplified manipulation. At the same time, the analysis highlights the Act's potential and its shortcomings in addressing this fast-moving threat landscape.

2. Disinformation meets AI: Definitions and Regulatory Tensions.

Disinformation involves the intentional creation and the spread of content that is demonstrably false or misleading. Disinformation is designed to deceive the public and potentially inflict harm.[6] However, its objective is not always to persuade but often to disrupt, to erode trust and social consensus, and to weaken democratic institutions. One example emerged during the COVID-19 pandemic, when coordinated efforts to falsely link the spread of the virus to 5G technology gained traction online.[7] These claims had no scientific basis, but they circulated widely on social media. They prompted vandalism of telecom infrastructure in several countries, and they contributed to public confusion at a time that was critical. Among the elements that set AI-driven disinformation apart from earlier forms, we can mention its scale, speed, and precision. Today's disinformation is powered by generative AI and deep learning models; it can be produced rapidly, while it can achieve high levels of realism and emotional appeal. The tools of 'deepfakes', i.e. hyper-realistic audio or video forgeries, have already been used to impersonate public figures, but also to interfere with elections, as well as to fabricate evidence of atrocities. These tools can mimic voices, facial expressions, and writing styles, leading the public to question the

[4] S Bond, 'How AI Deepfakes Polluted Elections in 2024' (NPR, 21 December 2024) <https://www.npr.org/2024/12/21/nx-s1-5220301/deepfakes-memes-artificial-intelligence-elections> accessed 11 July 2025.

[5] T Davina, 'GE2025: Surge in AI-Generated Videos Related to Elections after Polls Called' (CNA, 23 April 2025) <https://www.channelnewsasia.com/singapore/ge2025-deepfakes-ai-generated-tiktok-politicians-disinformation-5078011> accessed 11 July 2025.

[6] D Fallis, 'What Is Disinformation?' (2015) 63 Library Trends 401; E Kapantai and others, 'A Systematic Literature Review on Disinformation: Toward a Unified Taxonomical Framework' (2021) 23 New Media & Society 1301.

[7] A Bruns, S Harrington and E Hurcombe, '"Corona? 5G? Or Both?": The Dynamics of COVID-19/5G Conspiracy Theories on Facebook' (2020) 177 Media International Australia 12.

authenticity of images, videos, and even first-hand accounts. In one instance, a 2022 video appeared online showing Ukrainian President Volodymyr Zelensky announcing his surrender to Russian forces. The video was unconvincing and easy to debunk, but it was shared across numerous social platforms and their users. This highlights how synthetic content, even at lower quality, can be weaponised to confuse the public and distort the understanding of political and military events.[8]

The spread of AI-generated content can be accelerated by algorithmic curation, which influences what users encounter online. The problem is that social media platforms depend on recommendation algorithms that prioritise engagement. This means that they often elevate content that provokes strong emotional reactions (outrage, fear, or humour), without regard for truthfulness. Therefore, emotionally charged disinformation is more likely to be surfaced and shared, while accurate but less sensational information may be overlooked by the social media platforms.[9] This creates an environment where falsehoods are likely to outperform factual content, not because they are more convincing, but because their provocative nature is favoured by platform algorithms.[10] Over time, such patterns can distort collective understanding, promote polarized approaches, and diminish trust in authoritative sources. A striking example occurred in the aftermath of the 2023 earthquake in Turkey and Syria. Social media feeds were filled with AI-generated images depicting destroyed buildings and suffering civilians.[11] Many of these were circulated by accounts aiming to attract attention, clicks, or even fraudulent donations. Despite their lack of authenticity, the emotional impact of these visuals led to widespread engagement, which often outpaced the reach of verified updates from emergency services. This underscores how generative AI, when paired with algorithmic amplification, can be exploited during crises to mislead the public.

At the regulatory level, legal systems are confronted with the difficult task of finding the right balance. Disinformation poses a threat to democratic dialogue, social cohesion, and public safety. It can fuel hatred, provoke violence, as well as manipulate public opinion through coordinated campaigns.[12] Yet, efforts to regulate disinformation carry risks too, such as the risk of overreach and the risk of suppressing lawful expression. This is especially problematic in areas where concepts such as "falsehood," "harm," or "public interest" are subjective and politically charged.[13] The legal challenge in this context lies in distinguishing between deliberate manipulation and honest mistake, and in designing responses that address the underlying intent of

[8] J Wakefield, 'Deepfake Presidents Used in Russia-Ukraine War' (*BBC*, 18 March 2022) <https://www.bbc.com/news/technology-60780142> accessed 11 July 2025.
[9] J Serrano-Puche, 'Digital Disinformation and Emotions: Exploring the Social Risks of Affective Polarization' (2021) 31 International Review of Sociology 231.
[10] N Bontridder, Y Poullet, 'The Role of Artificial Intelligence in Disinformation' (2021) 3 Data & Policy e32.
[11] S Khatsenkova, 'What's Real and What's Fake: Debunking Misleading Content about the Turkey Earthquake' (Euronews, 2 July 2023) <https://www.euronews.com/2023/02/07/whats-real-and-whats-fake-debunking-misleading-content-about-the-turkey-earthquake> accessed 10 July 2025.
[12] S McKay, C Tenove, 'Disinformation as a Threat to Deliberative Democracy' (2021) 74 Political Research Quarterly 703.
[13] L Gielow Jacobs, 'Freedom of Speech and Regulation of Fake News' (2022) 70 The American Journal of Comparative Law i278.

disinformation, rather than punishing those who merely share inaccurate or controversial views. A credible regulatory approach must focus on systemic harms, such as the algorithmic amplification of coordinated inauthentic behaviour or the orchestration of state-sponsored influence campaigns. At the same time, it must also preserve core rights, including freedom of expression, media pluralism, and political dissent.[14] France provides an interesting case study. In 2018, it enacted legislation aimed at curbing "manipulation of information" in the run-up to elections.[15] The provisions of that law empower courts to block or remove content deemed false and deliberately spread at scale within three months of a national vote. The measure was introduced to safeguard electoral integrity, but it has raised serious concerns and criticism from journalists, academics, and civil society groups, who argue that its vague terms risks enabling excessive state control over political speech.[16] The French example highlights the ongoing tension between countering manipulation and preserving the openness and contestation that are very important for democratic life.[17]

3. Regulatory Tools in the EU AI Act for Combating AI-Driven Disinformation.

The EU AI Act,[18] formally adopted in 2024, is the EU's flagship regulatory response to the opportunities and risks posed by AI systems.[19] The AI Act introduces a risk-based approach to AI governance and it classifies systems into four tiers: unacceptable risk (prohibited), high-risk, limited risk, and minimal risk.[20] The AI Act applies both to providers (those who develop AI systems) and deployers (those who use them), including public and private entities. Moreover, the scope of the AI Act is horizontal, cutting across sectors, and includes general-purpose AI models (GPAI), which is a class particularly relevant for disinformation concerns. Although the Act does not explicitly target disinformation, its architecture includes tools that can mitigate disinformation's supply chains and propagation mechanisms, particularly when powered by GPAI. Some sets of provisions are of particular relevance. First, there are provisions that address GPAI, including foundation models and

[14] F Nuñez, 'Disinformation Legislation and Freedom of Expression' (2020) 10 UC Irvine Law Review 783.
[15] I Couzigou, 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression' (2021) 20 Election Law Journal: Rules, Politics, and Policy 98.
[16] A Harcourt, 'Legal and Regulatory Responses to Misinformation and Populism' in T Howard and S Waisbord (eds), *The Routledge Companion to Media Disinformation and Populism* (Routledge 2021); MR Fiorentino, 'France Passes Controversial "fake News" Law' (*Euronews*, 22 November 2018) <https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law> accessed 11 July 2025.
[17] C Marsden, T Meyer and I Brown, 'Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation?' (2020) 36 Computer Law & Security Review 105373.
[18] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (2024/1689).
[19] G Pavlidis, 'Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI' (2024) 16 Law, Innovation and Technology 293.
[20] M Ebers, 'Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act' [2024] European Journal of Risk Regulation 1.

generative AI systems such as large language models.[21] Second, there are prohibitions for specific AI practices deemed incompatible with Union values, including manipulative techniques that exploit vulnerabilities.[22] Finally, there are post-market monitoring and enforcement mechanisms, which aim to ensure continued compliance and adapt to emerging risks.[23]

The AI Act introduces obligations for providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union. These obligations are imposed to providers irrespective of whether they are established or located within the Union or in a third country.[24] The term 'provider', as defined in Article 2(3) of the Act, refers to a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model. The Act also applies to deployers of AI systems that have their place of establishment or are located within the Union, as well as to providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union. The term 'deployer', as defined in Article 2(4) of the Act, means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity. Moreover, the Act covers importers and distributors of AI systems, product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark. Authorised representatives of providers, which are not established in the Union also covered.

Key requirements under the AI Act include disclosure that the content has been generated by AI, technical documentation on the training data, architecture, and performance, as well as the implementation of safeguards to prevent the generation of illegal content.[25] The Act creates distinct obligations for providers and deployers; nevertheless, the line between them can blur in the context of disinformation. For example, a malicious actor using a public API of an LLM to mass-generate election propaganda could be technically classified as a deployer. However, such person would exert de facto control over the outputs. Currently, most obligations fall on providers, while deployers remain lightly regulated, unless their use of the AI system can be qualified as high-risk. This seems to create an accountability gap, particularly for malicious or negligent uses of GPAI in campaigns of disinformation.

For its part, Article 50 (2) of the AI Act requires providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, to ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or

[21] OJ Gstrein, A Zwitter and N Haleem, 'General-Purpose AI Regulation and the European Union AI Act' (2024) 13 Internet Policy Review 1.
[22] RJ Neuwirth, 'Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)' (2023) 48 Computer Law & Security Review 105798.
[23] J Mokander and others, 'Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation' (2022) 32 Minds and Machines 241.
[24] M Czerniawski, 'Towards the Effective Extraterritorial Enforcement of the AI Act' in Jaap-Henk Hoepman and others (eds), *Privacy Symposium* 2024 (Springer Nature Switzerland 2025).
[25] N Díaz-Rodríguez and others, 'Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation' (2023) 99 Information Fusion 101896.

manipulated. This is important given the proliferation of AI systems capable of producing vast quantities of synthetic content poses a challenge to the integrity of the information environment. As these systems advance, one can expect that the output would become increasingly indistinguishable from human-created content. This would exacerbate the risks of misinformation, large-scale manipulation, fraud, impersonation, and consumer deception. For this reason, it is important to require providers of AI systems, particularly those capable of generating or manipulating content, to incorporate technical solutions that allow the machine-readable identification of outputs that have been generated or modified by AI. These solutions may include watermarks, metadata tagging, cryptographic provenance methods, logging, or other appropriate techniques. [26] To be effective, such tools must be reliable, interoperable, and technically robust, while also adaptable to different content types, the costs of implementation and the generally acknowledged state of the art, as required by Article 50(2) of the AI Act. Importantly, this requirement must not be intended to extend to assistive AI tools that perform standard editing functions without substantially altering the semantic content or structure of the input.

In addition to the obligations imposed on AI providers, those who deploy AI systems must also respect the principle of transparency when they use AI tools to generate or alter visual or audio content that closely mimics real people or events in a way that could mislead audiences into believing that the content is genuine. [27] Article 50(4) of the AI Act requires deployers to clearly and prominently label such content to indicate its AI origin. The obligation, however, is not absolute. It must be balanced against the need to protect freedom of expression and artistic freedom, particularly in cases involving satire, fiction, or creative uses that are clearly not intended to deceive. [28] In those cases, the transparency requirement may be fulfilled through disclosure methods that are appropriate to the use and do not interfere with the audience's experience or the expressive purpose of the work. A comparable duty of transparency may also apply to AI-generated or manipulated text, especially when the content is presented as informing the public on matters of general interest. That said, this obligation may be waived where the material has undergone human editorial review and there is a clearly identifiable person or organisation that assumes responsibility for its publication. [29]

While these transparency obligations are binding, their effective implementation may be promoted by Union-level codes of practice. Under Article 50(7) of the AI Act, the AI Office must facilitate the drawing up of such codes of practice, which will then be approved by the Commission as implementing acts. These codes of practice may include practical arrangements

[26] AI Act (n 18) recital 133.
[27] J Botha and H Pieterse, 'Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security' (presented at 15th International Conference on Cyber Warfare and Security, 2020) <https://www.researchgate.net/publication/341454354_Fake_News_and_Deepfakes_A_Dangerous_Threat_for_21st_Century_Information_Security> accessed 11 July 2025.
[28] R Cejudo, 'Ethical Problems of the Use of Deepfakes in the Arts and Culture' in F Lara and J Deckers (eds), *Ethics of Artificial Intelligence* (Springer Nature Switzerland 2023) <https://doi.org/10.1007/978-3-031-48135-2_7> accessed 11 July 2025.
[29] G Hu, 'Challenges for Enforcing Editorial Policies on AI-Generated Papers' (2024) 31 Accountability in Research 978.

for content detection, as well as mechanisms for flagging or verifying the authenticity of information. They may also include collaboration mechanisms among stakeholders across the content distribution chain. Such initiatives have the potential to increase the capacity of users and intermediaries to identify AI-generated content and assess its trustworthiness.[30]

These transparency obligations gain particular significance in view of the Digital Services Act (DSA)[31] and the systemic risks that the DSA identifies, particularly those that threaten democratic institutions, electoral integrity, and the quality of civic discourse. Mechanisms for labelling AI-generated content form part of the broader regulatory strategy of the EU that requires very large online platforms and search engines to identify and mitigate risks, including those posed by synthetic media. It is important to note that the transparency duties set out in the AI Act operate independently, without prejudice to the content moderation rules established by the DSA. The obligation to disclose that content is artificially generated is separate from the legal assessment of whether the content is unlawful. That assessment is made solely on the basis of the applicable standards governing illegality, not on the mere fact that the content in question originated from an AI system.

The AI Act also introduces explicit prohibitions on certain uses of AI. These prohibitions cover the deployment of subliminal techniques and manipulative systems that exploit the vulnerabilities of specific groups, as outlined in Article 5(1) of the AI Act. In principle, this prohibition could cover disinformation campaigns targeting minors or marginalised communities. However, the thresholds for what constitutes "manipulation" or "exploitation" under the Act are relatively high. This means that political deepfakes or emotionally charged narratives aimed at a broad audience could fall outside the scope of this prohibition. One might argue that such content could fall within Article 5(1) of the AI Act where it causes significant harm or is used in a targeted and systematic manner. Yet, there is a broader issue of legal classification. Most instances of AI-generated disinformation do not meet the criteria for "unacceptable risk" under the AI Act, while they do not clearly fall within the high-risk categories. As it stands, the AI Act seems to be more finely tuned to addressing technical harms, such as those arising from the use of AI in medical devices or biometric surveillance, than to the harms associated with the manipulation of information, which are more dependent on the context.

The AI Act introduces post-market monitoring obligations for AI systems, including mechanisms for incident reporting and the continuous updating of risk assessments. In theory, these mechanisms could help identify cases of disinformation. National supervisory authorities and the newly established European AI Office are entrusted with the tasks of oversight and coordination. However, the Act does not establish a clear mechanism for redress in cases where AI-generated disinformation harms reputations or disrupts electoral processes. Without specific provisions targeting disinformation, enforcement

[30] RM Ballardini, K He and T Roos, 'Chapter 8: AI-Generated Content: Authorship and Inventorship in the Age of Artificial Intelligence' in T Pihlajarinne, J Vesala and O Honkkila (eds), *Online Distribution of Content in the EU* (Edward Elgar Publishing 2019).

[31] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, 1–102.

is likely to remain reactive, relying on broader regulatory cooperation.

4. Legal Strategies Against AI-Fuelled Disinformation.

As previously noted, the DSA offers a complementary layer to the AI Act by addressing a different but still crucial dimension of the digital landscape: content dissemination. Whereas the AI Act regulates the design, development, and deployment of AI systems, particularly those classified as high-risk, the DSA focuses on how content is distributed and moderated across digital platforms. Under the DSA, Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)—those with more than 45 million users in the EU—are subject to specific due diligence obligations.[32] These include mandatory risk assessments, algorithmic transparency, data access for vetted researchers, and independent audits, especially in relation to systemic risks. These risks include disinformation, algorithmic manipulation, and threats to democratic discourse. In the context of the EU regulatory approach, the DSA addresses the amplification and circulation of content in online spaces, while the AI Act governs how such content might be synthetically generated. When applied together, the two legislative instruments seek to address both the creation and the rapid spread of AI-driven disinformation. Nonetheless, there are still important regulatory gaps. Coordination between enforcement authorities (the European Commission, national Digital Services Coordinators,[33] and the newly created European AI Office) is not yet developed. Moreover, there are still questions around overlapping mandates, mechanisms for joint enforcement in cross-border cases, and coherent oversight of hybrid systems, which can merge generative AI technologies with large-scale infrastructures of content dissemination.

Some real-world scenarios can illustrate the intersection of the AI Act and the DSA. For example, a generative AI chatbot integrated into a VLOP could begin generating persuasive yet false claims about an emerging public health crisis. Since the platform's algorithms would amplify and disseminate this content to millions of users, the impact would become immediate and far-reaching. In such a case, the AI Act would apply to the AI provider, imposing technical safeguards such as output labelling, system traceability, and risk management procedures. At the same time, the DSA would require the platform to assess and mitigate the systemic risks posed by the spread of such disinformation, through transparency obligations, risk assessments, and possibly by modifying the content's algorithmic reach. In a second scenario, one could consider a political campaign using a generative AI tool to produce deepfake videos aimed at discrediting an opposing candidate. These videos could then spread through micro-targeted ads on a major social media

[32] B Genç-Gelgeç, 'Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies?' (2022) 18 Croatian Yearbook of European Law and Policy 25–60.

[33] P Van Cleynenbreugel and P Mattioli, 'Digital Services Coordinators and Other Competent Authorities in the Digital Services Act: Streamlined Enforcement Coordination Lost?' (European Law Blog, 30 November 2023) <https://www.europeanlawblog.eu/pub/digital-services-coordinators-and-other-competent-authorities-in-the-digital-services-act-streamlined-enforcement-coordination-lost/release/1> accessed 11 July 2025.

platform. In this case, the AI Act would impose obligations on the developer of the generative AI system, such as maintaining documentation, ensuring content authenticity, and preventing misuse. At the same time, the DSA would require the hosting platform to act swiftly, by removing or demoting harmful content and adjusting recommender systems, particularly in the lead-up to elections. These two examples highlight the need for coherent enforcement and coordination between the two regimes, particularly in scenarios where content creation and content dissemination are intertwined.

In addition to the DSA, the Code of Practice on Disinformation constitutes an important instrument aimed at combating online disinformation. Established in 2018, the Code was significantly strengthened in 2022, in order to be recognised as a Code of Conduct under the DSA. In February 2025, the Commission and the European Board for Digital Services endorsed the integration of the Code into the framework of the DSA.[34] The Code brings together a wide range of signatories, including online platforms and industry associations, as well as advertisers, fact-checkers, civil society organisations, and researchers. The Code contains numerous commitments and measures, covering various areas, from the demonetisation of disinformation and the transparency of political advertising to the empowerment of users and cooperation with fact-checkers. The Code is not legally binding, but it has become an integral part of the EU's regulatory framework, particularly under the DSA. For VLOPs and VLOSEs, adherence to the Code is recognised as a mitigation measure that demonstrates compliance with systemic risk management obligations under the DSA. For its part, the European Commission monitors the implementation of the Code through the Transparency Centre[35]. The newly established European Board for Digital Services[36] is also expected to play a coordinating role. The AI Act does not formally incorporate the Code of Practice, buts its transparency, traceability, and risk mitigation obligations, have the potential to support the Code's commitments. For example, requirements to label AI-generated content can support the Code's objectives on the traceability and authenticity of information. This would create meaningful synergies between the EU's voluntary and binding frameworks.

Article 11 of the EU Charter of Fundamental Rights[37] guarantees the right to freedom of expression and information, which sets the outer limits of both the AI Act and the DSA. Enforcement actions under these two instruments, particularly in the context of disinformation, content moderation, or transparency, must respect this fundamental right.[38] Importantly, freedom of

[34] European Commission, 'Commission Endorses the Integration of the Voluntary Code of Practice on Disinformation into the Digital Services Act' (2025) Press Release <https://digital-strategy.ec.europa.eu/en/news/commission-endorses-integration-voluntary-code-practice-disinformation-digital-services-act> accessed 11 July 2025.

[35] For more information, see 'Transparency Center' <https://disinfocode.eu/> accessed 11 July 2025.

[36] 'The European Board for Digital Services Is an Independent Advisory Group That Has Been Established by the Digital Services Act, with Effect from 17 February 2024. It Is Composed of the Member States' Digital Services Coordinators and Chaired by the European Commission. For more information see <https://digital-strategy.ec.europa.eu/en/policies/dsa-board> accessed 11 July 2025.

[37] Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407.

[38] A Kuczerawy, 'Fighting Online Disinformation: Did the EU Code of Practice Forget about Freedom of Expression?' in D Trottier and others (eds), *Disinformation and Digital Media as a Challenge for Democracy* (Intersentia 2020).

expression does not protect only the communication of factual information. It also covers satire, parody, artistic creation, political speech, and the airing of dissenting or minority views, even when such expression is controversial, provocative, or even offensive to some audiences. However, AI-generated content risks blurring the boundaries between expression and deception. In this context, regulatory responses to disinformation must be designed to avoid chilling legitimate speech, such as the use of AI tools to create parody videos, satirical memes, or artistic reinterpretations of public figures. If rules are applied too broadly or without flexibility, there is a risk of suppressing lawful content and content with cultural value.[39] For this reason, there is a need for a rights-sensitive approach to the implementation of the rules, while measures to combat disinformation should be precise and proportionate. The focus must remain on intentional deception and coordinated manipulation, not on the mere fact that the content is AI-generated.

A real-world example, which has been widely discussed, concerns the viral image of Pope Francis wearing a white puffer jacket, generated by an AI tool and circulated in 2023.[40] The image was not created with the intent to deceive or cause harm, but its realism raised concerns about the importance of watermarking and provenance technologies. Some advocated for mandatory labelling of all AI-generated content, but critics cautioned that such blanket requirements could limit harmless or humorous uses of AI, particularly in the realm of popular culture. For example, an activist group could produce a satirical video with generative AI, exaggerating a political leader's statements during an election campaign. This might be labelled "manipulated media" by some, but it could also qualify as protected political expression, especially if its satirical nature is apparent to a reasonable viewer. In such cases, regulators and platforms must distinguish between manipulative disinformation and lawful forms of expression, [41] including exaggeration and parody. Moreover, procedural safeguards are essential for upholding freedom of expression. Human review of flagged content, accessible appeals processes, and transparency reporting can help guard against censorship by proxy, whether through government mandates or algorithmic content moderation.[42] The AI Act's obligations on transparency and record-keeping must also be interpreted in a manner consistent with fundamental rights. They should not place a disproportionate burden on artists, journalists, or civil society actors who use AI tools for legitimate purposes in a creative or critical context.

[39] Nuñez (n 14).
[40] D Tolentino, 'AI-Generated Images of Pope Francis in Puffer Jacket Fool the Internet' (NBC News, 27 March 2023) <https://www.nbcnews.com/tech/pope-francis-ai-generated-images-fool-internet-rcna76838> accessed 11 July 2025.
[41] I Khan, 'A/HRC/47/25: Disinformation and Freedom of Opinion and Expression - Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' <https://www.ohchr.org/en/documents/thematic-reports/ahrc4725-disinformation-and-freedom-opinion-and-expression-report> accessed 11 July 2025.
[42] R Gorwa, R Binns and C Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 Big Data & Society 2053951719897945.

5. Critical Assessment and Future Directions.

The AI Act constitutes an important step forward in the EU's regulatory response to AI, but it is not a comprehensive solution to the problem of disinformation. Its provisions relevant to disinformation primarily address the supply side, i.e. the creation and dissemination of synthetic content. However, several key challenges remain. First, there is the problem of under-inclusiveness. There are many disinformation scenarios that fall outside the current classification framework of the AI Act. For instance, the malicious use of LLMs may not meet the thresholds for "high-risk" or "prohibited" systems under the AI Act, even when such use may cause real-world harm. Second, significant difficulties remain at the level of enforcement. Since disinformation is produced and distributed through opaque channels, it may be hard to trace specific outputs to a particular provider or deployer, particularly when open-source models or anonymised tools are involved.[43] Third, there is a problem of interpretative uncertainty. Key terms such as "manipulation," "transparency," and "exploitation" are open to legal and practical debate, and they are likely to remain contested. The precise meaning of these terms will need to be determined through regulatory guidance and the gradual development of case law.

Disinformation is not yet addressed through a unified legal framework at the EU level. The AI Act, the DSA, and the Charter of Fundamental Rights regulate different aspects of this fragmented landscape. There is a lack of dedicated regime targeting AI-driven misinformation risks, which risks opening the door to divergent national interpretations and enforcement across the EU Member States. Looking ahead, we argue that there is a need for a more integrated approach. This would involve aligning the enforcement of the AI Act with the systemic risk assessments under the DSA, as well as fostering technical interoperability through common standards for watermarking and metadata. This would also involve investing in complementary tools such as media literacy initiatives.[44] Such efforts should be supported by multi-stakeholder oversight structures that bring together regulators, civil society, and industry actors.

The AI Act is not crafted specifically to combat disinformation, but it introduces important tools, including transparency obligations, documentation requirements, and risk management processes. These tools can be used to address the supply side of synthetic and misleading content. To fight AI-driven disinformation, the EU must develop a rights-based, cross-cutting strategy that combines binding legal norms, soft governance frameworks, and technological safeguards. Moreover, effective implementation must be context-sensitive and transparent, seeking the delicate balance between safeguarding democratic integrity and upholding freedom of expression. As the fog of information continues to thicken, ensuring regulatory clarity is not merely a legal necessity: It is a democratic imperative.

---

[43] J Pielemeier, 'Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?' (2020) 2020 Utah Law Review 916.

[44] T Dame Adjin-Tettey, 'Combating Fake News, Disinformation, and Misinformation: Experimental Evidence for Media Literacy Education' (2022) 9 Cogent Arts & Humanities 2037229.

Maniaci A, 'Obbligo di riparazione del bene acquistato dal consumatore e sostenibilità' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252AM

EJPLT
ISSN 2704-8012

Obbligo di riparazione del bene acquistato dal consumatore e sostenibilità

Obligation to repair purchased goods by consumers and sustainability

ARTURO MANIACI
Professore Associato di Diritto Privato
Università degli Studi di Milano

Abstract

Nel saggio l'Autore, dopo aver ripercorso le origini della tutela ripristinatoria dell'acquirente e della nozione di durabilità, si sofferma ad analizzare alcune previsioni della dir. 2019/771/UE su taluni aspetti relativi ai contratti di vendita di beni ai consumatori, ritenendo, anche alla luce di altre fonti europee (fra cui la recente dir. 2024/1799/UE), che gli obiettivi euro-unitari dell'economia circolare, del consumo sostenibile e della tutela dell'ambiente sono destinati ad indurre giuristi e interpreti a configurare la sussistenza, in capo al professionista alienante, di un obbligo di riparazione dei beni non conformi, a fronte della richiesta di ripristino della conformità proveniente dal consumatore.

In the essay the Author, after retracing the origins of the purchaser's restorative protection and the notion of durability, dwells on analyzing some provisions of Directive 2019/771/EU on certain aspects concerning contracts for the sale of goods, considering, also in the light of other European sources of law (including, most recently, Directive 2024/1799/EU), that the European Union objectives of circular economy, sustainable consumption and environmental protection are bound to lead jurists and interpreters to configure a professional seller's duty to repair non-conforming goods, in the face of the consumer's request to have the good brought into conformity.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Consumer protection; sustainable development; circular economy; durability of goods; sales of goods; duty to repair

Summary: 1. Premessa: diritto privato e sostenibilità. – 2. Genesi della tutela ripristinatoria del compratore. – 3. Alle origini della 'durabilità' del bene oggetto di alienazione. – 4. La sostenibilità del mercato dei consumi nella Direttiva n. 2019/771/UE. – 5. La disciplina italiana di recepimento della Direttiva n. 2019/771/UE (D.lg. n. 170/2021) alla prova della sostenibilità. – 6. Verso una nuova semantica della tutela ripristinatoria: la riparazione del bene come oggetto di un obbligo gravante sull'alienante. – 7. Conclusioni.

1. Premessa: diritto privato e sostenibilità.

È indubbio che le regole del diritto privato, e segnatamente quelle dedicate alle garanzie dovute dall'alienante e alla tutela del consumatore-acquirente di beni mobili, possono contribuire, sia pure indirettamente, ad una gestione più efficiente delle risorse disponibili, al raggiungimento di obiettivi di sostenibilità ambientale[1] e, in definitiva, alla transizione verso un modello di economia circolare[2], oggi normativamente definito a livello euro-unitario come «un sistema economico in cui il valore dei prodotti, dei materiali e delle altre risorse nell'economia è mantenuto il più a lungo possibile, migliorandone l'uso efficiente nella produzione e nel consumo, così da ridurre l'impatto ambientale del loro uso, riducendo al minimo i rifiuti e il rilascio di sostanze pericolose in tutte le fasi del loro ciclo di vita, anche mediante l'applicazione della gerarchia dei rifiuti» (art. 2, § 1, n. 9 Reg. UE n. 2020/852, noto come 'Regolamento Tassonomia').

Nelle pagine che seguono ci proponiamo di verificare, in particolare, se ed eventualmente in che misura la disciplina euro-unitaria della vendita mobiliare sia idonea a realizzare le finalità sottese ad un consumo sostenibile, il quale reclama, *inter alia*, che gli strumenti e le forme di tutela civile siano impiegate

[1] Sulle radici e sull'evoluzione della formula dello 'sviluppo sostenibile' (che ricorre in diversi trattati europei e condensa uno degli obiettivi principali dell'Unione europea), v. D. IMBRUGLIA, *Mercato unico sostenibile e diritto dei consumatori*, in *Persona e Mercato*, 2021, 3, 496 ss.; M. PIERACCINI, T. NOVITZ, *Sustainability through History*, in M. Pieraccini, T. Novitz, *Legal Perspectives on Sustainability*, Bristol, 2020, 9 ss.; S. LANDINI, *Clausole di sostenibilità nei contratti tra privati. Problemi e riflessioni*, in *Dir. pubbl.*, 2015, 614 ss. Il sintagma ha già fatto ingresso anche nel discorso legislativo domestico (v. ad es. art. 3-*quater* d.lg. n. 152/2006, introdotto dal d.lg. n. 4/2008, che eleva lo sviluppo sostenibile a principio fondamentale della disciplina in materia ambientale). Si discorre, poi, già di 'analisi ecologica' del diritto privato o del diritto contrattuale (M. KÜHN, *Umweltschutz durch Privatrecht. Eine Studie zur ökologischen Analyse der privatrechtlichen Schutzrechte und des Vertragsrechts in Deutschland und England*, Frankfurt a.M., 2007; I. BACH, E.M. KIENINGER, *Ökologische Analyse des Zivilrechts*, in *JZ*, 2021, 1088 ss.; da noi, cfr. soprattutto AA.VV., *Contratto e ambiente. L'analisi "ecologica" del diritto contrattuale*, a cura di M. PENNASILICO, Napoli, 2016).

[2] Sul passaggio dall'economia lineare a quella circolare quale nuovo paradigma della sostenibilità, cfr., *ex multis*, M. MELI, *Oltre il principio chi inquina paga: verso un'economia circolare*, in *Riv. crit. dir. priv.*, 2017, 73 ss.; A.C. NAZZARO, *Rifiuti, beni e proprietà nella prospettiva dell'economia circolare*, in *Rass. dir. civ.*, 2020, 621 ss.; M. PENNASILICO, *Economia circolare e diritto: ripensare la "sostenibilità"*, in *Persona e Mercato*, 2021, 4, 718 ss.; S. VERNILE, *Dall'economia circolare al principio di circolarità. Una lettura giuridica nel solco dell'art. 9 Cost.*, Torino, 2024, 62 ss. e 225 ss.

e piegate in modo da ridurre quanto più possibile l'impatto dell'attività d'impresa sull'ecosistema ambientale del pianeta.

2. Genesi della tutela ripristinatoria del compratore.

La versione originaria del testo del Codice civile del 1942 – così come di altri codici civili europei di origine latina – rivela certamente il peso ereditato dalla tradizione romanistica, inveratasi nel modello di stampo edilizio, in base al quale la tutela del compratore di un bene affetto da determinate anomalie si articola (epperò al contempo si risolve ed esaurisce) nelle azioni redibitoria ed estimatoria (o *quanti minoris*) (art. 1492 c.c.), salva la possibilità di esperire un'azione risarcitoria per i danni subiti in relazione ai vizi del bene alienato (art. 1494 c.c.).

Sembrerebbe, dunque, estranea alla mentalità del legislatore italiano del 1942 l'idea di un rimedio volto a conseguire una ripetizione dell'adempimento del (*rectius*, una piena e perfetta realizzazione del complessivo risultato programmato nel) contratto di compravendita, consistente nella facoltà del compratore di chiedere all'alienante una regolarizzazione della prestazione traslativa, sicché riparazione e sostituzione, quali modi (*rectius*, rimedi) attraverso cui guadagnare il ripristino della conformità al contratto, sarebbero diventati nuovi requisiti dell'attribuzione traslativa soltanto per effetto dell'impulso del diritto europeo dei contratti di consumo.

Ma già la Codificazione prussiana del 1794 (*ALR*)[3] aveva attribuito (I, 5, §§ 325, 326 e 331) a favore del compratore un'azione di esatto adempimento *sub specie* di riparazione, e soltanto in subordine, qualora il venditore non fosse stato in grado di soddisfare la richiesta volta alla eliminazione del vizio o alla integrazione della qualità promessa mancante, l'azione redibitoria o estimatoria, che avevano, quindi, un ruolo sussidiario[4].

Analogamente, il Codice civile austriaco (lo *ABGB*) del 1811[5], la cui disciplina fu estesa ai territori del Regno Lombardo-Veneto dal 1816, aveva previsto (§§ 932 e 933), nel caso in cui il vizio del bene fosse eliminabile e tale da non impedire l'uso ordinario del bene, (l'esperibilità del)l'azione di esatto adempimento in alternativa alla *quanti minoris*[6].

Anche sotto il vigore del *Code civil* napoleonico del 1804, e cioè sotto il vigore del codice che più di ogni altro è debitore della tradizione romanistica, i formanti giurisprudenziale e dottrinale avevano tentato di superare le strettoie

---

[3] Circa le ragioni per le quali l'*ALR* non rappresentò un modello per le successive codificazioni europee, cfr. C.A. Cannata, *Legislazione, prassi, giurisprudenza e dottrina dal XVIII al XX secolo come premesse per l'avvenire del diritto privato europeo*, in Aa.Vv., *Nozione formazione e interpretazione del diritto dall'età romana alle esperienze moderne. Ricerche dedicate al Professor Filippo Gallo*, III, Napoli, 1997, 26.

[4] Sul punto, cfr. *amplius* R. Calvo, *Vendita e responsabilità per vizi materiali*, II, *Il regime delle «garanzie» nelle vendite al consumo*, Napoli, 2007,198 ss., che intende il rimedio come volto ad ottenere una '*restitutio in integrum*'.

[5] Sull'influenza del modello asburgico in Italia, cfr. E. Dezza, *Lezioni di storia della codificazione civile. Il* Code Civil *(1804) e l'*Allgemeines Bürgerliches Gezeztbuch *(ABGB, 1812)*, 2ª ed., Torino, 2000, 160 ss.

[6] Maggiori ragguagli in: L. Garofalo, *Le azioni edilizie e la Direttiva 1999/44/CE*, in AA.VV., *Strutture e forme di tutela contrattuali*, a cura di V. Mannino, Padova, 2004, 134 ss.; S. Cherti, *La vendita dei beni di consumo e la nozione di riparazione*, in *Europa e dir. priv.*, 2003, 706 ss.; R. Calvo, *Vendita e responsabilità per vizi materiali*, II, cit., 201 ss.

poste da quello legale (cfr. artt. 1641-1649), pervenendo a riconoscere il diritto del compratore alla riparazione della cosa venduta: il primo, attraverso l'espediente dell'*astreinte*[7]; il secondo, considerandola una conseguenza – sia pure subordinata alla ricorrenza del presupposto della possibilità (avendo sotto tale profilo riguardo soprattutto al rapporto di proporzionalità fra i costi che comporta la riparazione ed il valore della cosa) – dei principi e delle norme generali, la cui applicabilità non è esclusa dall'art. 1644 del *Code civil*[8].

A risultati non dissimili da quelli raggiunti dalla dottrina e dalla giurisprudenza francesi era pervenuta la dottrina italiana nel vigore del Codice civile del 1865, il quale in materia di vendita – riproducendo fedelmente le norme del Codice civile francese – aveva contemplato esclusivamente le azioni redibitoria e *quanti minoris* (nel senso che al compratore era accordata la facoltà di scelta fra «rendere la cosa e farsi restituire il prezzo» ovvero «ritenerla e farsi restituire quella parte di prezzo che sarà determinata dall'autorità giudiziaria»: art. 1501), ma ove era in termini generali previsto che «la parte verso cui non fu eseguita l'obbligazione, ha la scelta o di costringere l'altra all'adempimento del contratto, quando sia possibile, o di domandarne lo scioglimento, oltre il risarcimento dei danni in ambedue i casi» (art. 1165)[9].

Nell'ordinamento tedesco, la riparazione della cosa difettosa, pur non essendo originariamente contemplata dal *BGB*, era divenuta un onere del venditore per effetto della successiva *Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen* (*AGB-Gesetz*) del 9 dicembre 1976, entrata in vigore il 1° aprile 1977, la quale annoverava (§ 11, n. 10, lett. *b*) nella c.d. *black list* delle clausole assolutamente inefficaci la clausola, inserita nei contratti aventi ad oggetto la fornitura di merci di nuova produzione, con la quale si fosse limitata, totalmente o parzialmente, la garanzia ad un diritto alla riparazione, qualora non fosse stato espressamente riservato al compratore il diritto alla riduzione del prezzo o a sua scelta alla risoluzione del contratto nel caso di mancata riuscita (*scilicet*: rifiuto, ritardo o impossibilità) della riparazione.

Il Codice civile olandese (*OBW*), nella versione antecedente all'entrata in vigore del nuovo Codice civile (*NBW*) del 1992, attribuiva all'acquirente di un bene di consumo il diritto alla sostituzione o riparazione della cosa venduta: «Beantwoordt het afgeleverde niet aan de overeenkomst, dan kan de koper

---

[7] Come documentato da G. Gorla, *Considerazioni in tema di garanzia per i vizi redibitori*, in *Riv. trim. dir. e proc. civ.*, 1957, 1278, nota 7.

[8] G. Baudry-Lacantinerie-L. Saignat, *Traité théorique et pratique de droit civil*, *De la vente et de l'échange*, 3ª ed., Paris, 1908, n. 434, 452. In senso conforme, cfr. anche la dottrina (francese) menzionata da J. Limpens, *La vente en droit belge*, Bruxelles-Paris, 1960, n. 400, 174 e da C. Aubry e C.F. Rau, *Cours de droit civil français d'après la méthode de Zachariae*, 5ª ed., t. V, Paris, 1907, § 355 *bis*, 113, nota 14 *bis*; più di recente, J. Ghestin, *Conformité et garanties dans la vente (Produits mobiliers)*, Paris, 1983, 45, 48 e 163; J. Viney, *Les condamnations à exécuter ou à réparer en nature*, in J. Viney et P. Jourdain, *Les effets de la responsabilité,* 2ª ed., nel *Traité de droit civil*, dir. da J. Ghestin, Paris, 2001, 31 ss.

[9] Con specifico riferimento alla vendita, ritenevano ammissibile un'azione di esatto adempimento, nel caso in cui l'oggetto del contratto fosse una cosa determinata solo nel genere, pur con diverse sfumature, C. Vivante, *Trattato di diritto commerciale*, IV, *Le obbligazioni*, Milano, 1926, n. 1676, 166, valorizzando gli usi commerciali; C.L. Gasca, *Trattato della compra-vendita civile e commerciale*, 2ª ed., II, Torino, 1915, n. 1314, 907; G. Scaduto, *L'*exceptio non adimpleti contractus *nel diritto civile italiano*, in *Annali del Seminario giuridico della R. Università di Palermo*, VIII, Palermo, 1921, 90; A. Ramella, *La vendita nel moderno diritto*, I, Milano, 1920, 447-448 (a condizione che il venditore fosse artefice o produttore della cosa difettosa e che la riparazione fosse possibile entro breve tempo). Anche la giurisprudenza aveva in qualche occasione ritenuto ammissibile una tutela ripristinatoria, ove il venditore si fosse offerto di riparare il bene (App. Bologna, 23 dicembre 1929, in *Rep. Foro it.*, 1930, voce "Vendita", n. 214).

eisen: a. aflevering van het ontbrekende; b. herstel van de afgeleverde zaak, mits de verkoper hieraan redelijkerwijs kan voldoen; c. vervanging van de afgeleverde zaak, tenzij de afwijking van het overeengekomene te gering is om dit te rechtvaardigen, dan wel de zaak na het tijdstip dat de koper redelijkerwijze met ongedaanmaking rekening moet houden, teniet of achteruit is gegaan doordat hij niet als een zorgvuldig schuldenaar voor het behoud ervan heeft gezorgd» (art. 7:21)[10].

Anche altri codici civili europei, più o meno riconducibili al modello franco-tedesco, come quello portoghese (cfr. art 914 *Código Civil*), greco (cfr. art. 559, primo periodo, *AK*) e svizzero (cfr. artt. 206 e 368, 2° co., *CO*)[11], nonché la maggior parte dei sistemi giuridici appartenenti all'area dell'estremo Nord europeo (in particolare: quelli scandinavi), non propriamente collocabili nell'alveo delle due macro-famiglie giuridiche di *Civil Law* e di *Common Law*, ma notoriamente all'avanguardia in materia di tutela del consumatore, riconoscevano – a determinate condizioni – il diritto del compratore alla sostituzione o riparazione della cosa acquistata.

Ma anche nel Codice civile italiano del 1942 non manca(va)no indici che depongono nel senso dell'ammissibilità di recupero del risultato traslativo avuto di mira dai contraenti in un momento successivo al trasferimento e alla consegna del bene.

Fermo restando quanto già previsto in tema di compravendita dall'art. 1512 c.c. (secondo cui, quando in forza di un apposito patto o in base agli usi il venditore assuma per un determinato tempo la garanzia di buon funzionamento del bene venduto, il compratore vanta anche il diritto di chiedere la riparazione o sostituzione del bene), e quanto previsto in tema di appalto dall'art. 1668 c.c. (applicabile anche al contratto d'opera in forza dell'espresso rinvio operato dall'art. 2226, 3° co., c.c. e al contratto di costruzione di nave o di aeromobile in forza del richiamo contenuto rispettivamente negli artt. 241 e 856 c. nav.), una parte consistente della dottrina era già pervenuta a ritenere ammissibile in termini generali una pretesa alla riparazione o alla sostituzione del bene affetto da anomalie strutturali che incidono sulla sua utilizzabilità o sul suo valore economico, vuoi desumendo un principio generale dalle disposizioni testé prefate, vuoi sulla base delle norme generali in tema di risoluzione del contratto per inadempimento di cui agli artt. 1453 e ss. c.c., vuoi qualificando quella pretesa come azione di risarcimento del danno in forma specifica ex art. 2058 c.c., vuoi

---

[10] Sul punto, cfr. A.J.B. Sirks, *Die Umsetzung der Richtlinie 1999/44/EG in den Niederlanden*, in Aa.Vv., *Verbraucherkauf in Europa*, a cura di M.J. Schermaier, München, 2003, 280; E. Hondius-C. Jeloschek, *Die Kaufrichtlinie und das niederländische Recht: Für den Westen kaum etwas Neues*, in Aa.Vv., *Europäisches Kaufgewährleistungsrecht. Reform und Internationalisierung des deutschen Schuldrechts*, a cura di S. Grundmann-D. Medicus-W. Rolland, Köln, 2000, 210 ss.

[11] Vero che in materia di compravendita il Codice svizzero delle obbligazioni prevede espressamente soltanto il rimedio della sostituzione di cose di genere (art. 206 *CO*) e che il rimedio della riparazione è invece contemplato in materia di contratto d'opera (art. 368, 2° co., *CO*). Vero è anche, però, che la dottrina ritiene che tale ultima disposizione sia analogicamente applicabile alla compravendita (T. Guhl, A. Koller, *Das Schweizerische Obligationenrecht*, 9ª ed., Zürich, 2000, § 42, Rn. 48), o comunque che l'obbligo del venditore di riparare la cosa discenda dal principio di buona fede (H. Honsell, *Schweizerisches Obligationenrecht, Besonderer Teil*, 6ª ed., Bern, 2001, 92).

invocando la clausola generale di buona fede contrattuale di cui all'art. 1375 c.c.[12].

Dal canto suo, la giurisprudenza ha in passato accordato al venditore il diritto (*rectius*, la facoltà) di scegliere di riparare o sostituire il bene al fine di evitare le conseguenze derivanti dall'accoglimento del rimedio redibitorio[13]. Anzi, in alcune occasioni ha financo ravvisato nel rifiuto, da parte del compratore, dell'offerta del venditore di provvedere a riparare il bene una circostanza idonea ad escludere la risoluzione del contratto[14], facendo così in un certo senso applicazione – non si sa con quale grado di consapevolezza – dell'istituto dell'*exceptio doli generalis*.

Merita, infine, di essere ricordato che, ancor prima che prendesse l'abbrivo il processo di edificazione europea del diritto dei consumatori, era stata affrontata la questione se il venditore avesse l'obbligo di mantenere e fornire al compratore i pezzi di ricambio necessari o utili al funzionamento del bene acquistato (come, ad esempio, una macchina), e un'autorevole voce della dottrina italiana era pervenuta a configurare in questi casi una prestazione accessoria dell'alienante, sostenendo che su quest'ultimo gravasse implicitamente – in virtù dell'affidamento che la parte acquirente riponeva in relazione ai costumi del traffico – anche l'impegno di fornire per il tempo di durata normale del bene i pezzi di ricambio fabbricati dall'alienante medesimo[15].

In definitiva, già da tempo una tutela ripristinatoria a favore di chi avesse acquistato una cosa affetta da anomalie era prevista da molti ordinamenti europei e aleggiava (quantomeno) nell'ordinamento giuridico italiano.

3. Alle origini della 'durabilità' del bene oggetto di alienazione.

Se (è pacifico che) nella nozione tecnico-giuridica di vizio redibitorio (art. 1490 c.c.) o di mancanza di qualità promesse o essenziali (art. 1497 c.c.) rientrano tutte quelle imperfezioni, inesattezze o difetti relativi al processo di produzione, fabbricazione, formazione e conservazione della cosa che influiscono sull'uso cui sarebbe destinata o ne diminuiscono in modo apprezzabile il valore, ovvero la mancanza di tutti quegli elementi essenziali e

---

[12] Per una sintesi delle diverse posizioni assunte sul tema, cfr. F. MACARIO, voce *Vendita. I) Profili generali*, in *Enc. giur. Treccani*, Roma, 1994, 30-31; A. PLAIA, *Sull'ammissibilità dell'azione di esatto adempimento in presenza di vizi del bene venduto o promesso in vendita*, in *Contr. e impr.*, 1998, 123 ss.; R. FADDA, *La riparazione e la sostituzione del bene difettoso nella vendita (dal codice civile al codice del consumo)*, Napoli, 2007, 107 ss.

[13] Cass. 11.5.1983, n. 3257, in *Rep. Foro it.*, 1983, voce "Vendita", n. 73. Nel panorama della giurisprudenza di merito, cfr. le sentenze citate da G. MUSUMECI, *Sui presupposti dell'azione di risoluzione nell'appalto e nella vendita*, in *Giur. it.*, 1993, I, 1, 1125, nota 17.

[14] Cass. 22.12.1977, n. 5701, in *Rep. Foro it.*, 1977, voce "Contratto in genere", n. 260.

[15] C.M. BIANCA, *La vendita e la permuta*, 2ª ed., in *Tratt. Vassalli*, VII, t. 1, *, Torino, 1993, 249. Segnaliamo, peraltro, che il Libro Verde sulle garanzie dei beni di consumo e dei servizi post-vendita, presentato dalla Commissione europea il 15 novembre 1993 (che ha preceduto i lavori di elaborazione della prima fonte normativa euro-unitaria in materia di garanzie nelle vendite mobiliari al consumatore), aveva escluso un obbligo siffatto in capo al venditore: «Any requirement to provide spare parts imposed exclusively on vendors is both unjust and ineffective. It is unjust because it places on the vendor a burden which he cannot shoulder on his own in a domain over which he has little say. It is ineffective because the vendor simply cannot be made entirely responsible, either for providing spare parts or for informing the consumer in this respect».

sostanziali idonei ad influire sull'appartenenza ad tipo o ad una specie diversa da quelli dedotti nel contratto[16], il difetto occulto di funzionamento dovuto ad una predeterminazione artificiale, da parte del produttore, della durata di utilizzo o di godimento di un prodotto tale da rendere il ciclo fisiologico di vita di quest'ultimo inferiore rispetto a quello che normalmente presenta un prodotto del medesimo tipo o della medesima specie avrebbe potuto *in thesi* legittimare l'acquirente all'esperimento dei c.d. rimedi edilizi previsti in tema di compravendita di diritto comune (art. 1492 c.c.) nei confronti del venditore, a prescindere da qualsivoglia giudizio di ascrivibilità di tale difetto a quest'ultimo a titolo di colpa. Del resto, come si è visto, è lo stesso legislatore del Codice civile del 1942 a prevedere (art. 1512 c.c.) che il venditore può impegnarsi ad assicurare al compratore una determinata durata di vita del bene, attraverso la stipulazione di una garanzia c.d. di buon funzionamento[17]: ciò conferma che nella nozione di funzionalità del bene rientra anche la sua idoneità a durare nel tempo, la quale può dunque concorrere a delineare una delle qualità del bene e, in definitiva, la prestazione dovuta dall'alienante.

Tuttavia, salve alcune sporadiche e occasionali prese di posizione dottrinale, il fenomeno della c.d. obsolescenza programmata (o precoce)[18] non è stato ricondotto entro i confini dello statuto delle garanzie nella vendita fino a quando il tema non ha formato oggetto di studi, dibattiti, proposte e iniziative in sede europea, in concomitanza con l'avvio ufficiale della strategia messa in atto negli ultimi anni dalle istituzioni europee per realizzare una maggiore sostenibilità ambientale e per favorire la transizione verso un'economia sempre più circolare[19]: strategia che sul terreno della patologia degli scambi individuali ha avuto come momento normativo apicale il superamento della Direttiva n. 1999/44/CE su taluni aspetti della vendita e delle garanzie dei beni di consumo ad opera delle nuove Direttive n. 2019/770/UE e 2019/771/UE.

Eppure, la Direttiva europea n. 1999/44/CE, nel dettare le regole integrative o suppletive che concorrono a declinare i criteri di conformità al contratto del bene oggetto di alienazione[20], contemplava (art. 2, § 2, lett. *d*) «la qualità e le prestazioni abituali di un bene dello stesso tipo, che il consumatore può ragionevolmente aspettarsi, tenuto conto della natura del bene e, se del caso, delle dichiarazioni pubbliche sulle caratteristiche specifiche dei beni fatte al riguardo dal venditore, dal produttore o dal suo rappresentante, in particolare

---

[16] Questo è il consolidato orientamento della giurisprudenza italiana (*ex multis*, v. Cass. 5.4.2016, n. 6596, in *Rep. Foro it.*, 2016, voce "Vendita", n. 29; Cass. 8.3.2013, n. 5845, in *Giur. it.*, 2013, 2495; Cass. 23.3.1982, n. 1839, in *Rep. Foro it.*, 1982, voce "Vendita", n. 52).

[17] Tant'è che G. Gorla, *La compravendita e la permuta*, in *Tratt. Vassalli*, Torino, 1937, 183 la qualificava «garanzia della durata, buon funzionamento o resistenza, della cosa per un determinato periodo di tempo», perché doveva garantire «una specifica qualità, la durata per quel dato tempo». Dal canto suo, la giurisprudenza ritiene essenziale la determinazione della durata, ai sensi e per gli effetti di cui all'art. 1512 c.c. (Cass. 18.7.1977, n. 3214, in *Giur. it.*, 1979, I, 1, 903; Cass. 29.5.1995, n. 6033, in *Rep. Foro it.*, 1995, voce "Vendita", n. 79).

[18] Una nozione di tale fenomeno si rinviene oggi a livello normativo euro-unitario nell'art. 2, § 1, n. 21 del Reg. UE n. 2024/1781, che stabilisce il quadro per la definizione dei requisiti di progettazione ecocompatibile per prodotti sostenibili (c.d. Regolamento ecodesign).

[19] Cfr. in particolare la Relazione della Commissione europea "*on the implementation of the Circular Economy Action Plan*", Brussels, 4.3.2019, COM(2019) 190 final.

[20] Nonostante il tenore letterale del testo della direttiva, non si trattava, infatti, di presunzioni in senso tecnico (G. Cian, *Presentazione*, in Aa.Vv., *L'attuazione della Direttiva 99/44/CE in Italia e in Europa. La tutela dell'acquirente di beni di consumo*, Padova, 2002, 12).

nella pubblicità o sull'etichettatura», sicché, in astratto, l'obsolescenza programmata del bene poteva già integrare gli estremi di un difetto di conformità, ove appunto si fosse tradotta nella lesione della ragionevole aspettativa del consumatore in determinate qualità o caratteristiche di durata e funzionalità del bene (confrontate con quelle di altri beni che rientrano nel medesimo genere merceologico), frutto di un'alterazione tecnica o tecnologica durante la fase di progettazione o produzione del bene[21], fermi restando, ovviamente, i problemi connessi quantomeno ai limiti temporali della garanzia di conformità (decadenza, prescrizione, durata della responsabilità del professionista-alienante) e agli oneri (di diligenza e probatori) gravanti sull'acquirente-consumatore[22].

Anche in assenza di regole specifiche sulla obsolescenza programmata dei prodotti di consumo, infatti, molti giuristi europei[23] non avevano escluso che il consumatore potesse in tali ipotesi far valere i rimedi previsti dalla disciplina euro-unitaria della vendita del 1999 in caso di difetto di conformità del bene acquistato (così, ad esempio, nell'ordinamento giuridico danese[24], spagnolo[25], belga[26], tedesco[27]).

In ogni caso, anche durante la vigenza della Direttiva n. 1999/44/CE, corrispondente ad un periodo temporale di venti anni, si rinvenivano ulteriori indici normativi che potevano deporre nel senso dell'attribuzione di rilevanza giuridica alla idoneità di certi prodotti a mantenere nel tempo le proprie caratteristiche funzionali.

Così, a titolo esemplificativo, la Direttiva n. 2009/125/CE del 21 ottobre 2009 relativa all'istituzione di un quadro per l'elaborazione di specifiche per la progettazione ecocompatibile dei prodotti connessi all'energia (abrogata dal Reg. UE 2024/1781, che stabilisce il quadro per la definizione dei requisiti di progettazione ecocompatibile per prodotti sostenibili) contemplava (v. Allegato I, 1.3, lett. *i*) una serie di parametri di progettazione ecocompatibile

---

[21] Come è stato rilevato, con l'introduzione dell'elemento dell'aspettativa del consumatore nella determinazione degli *standard* di qualità del bene scolora la distinzione fra prodotto e processo di produzione ai fini della responsabilità dell'alienante (H. COLLINS, *Conformity of Goods, the Network Society, and the Ethical Consumer*, in *ERPL*, 2014, 630: «Once the expectation of the buyer becomes the guiding thread for conformity, the distinction between the product itself and the process by which it was made becomes less significant, because the buyer's expectations may be addressed both to the functioning of the product and symbolic and expressive qualities that may include the manufacturing process»).

[22] Sul punto, sia consentito il rinvio ad A. MANIACI, *Rimedi e limiti di tutela dell'acquirente*, Pisa, 2018,133.

[23] Fra i quali, ad es., G. HOWELLS, C. TWIGG-FLESNER, T. WILHELMSSON, *Rethinking EU Consumer Law*, Abingdon-Oxon-New York, 2018, 183.

[24] M.J. SØRENSEN, *The Implementation of EU Directives 2019/770 and 2019/771/UE in Denmark*, in *EuCML*, 2022, 5, 200.

[25] R. PAZOS, *Sustainability, the Circular Economy and Consumer Law in Spain*, in *EuCML*, 5/2020, 215; cfr. anche J.A. SOTO PINEDA, *Reflexiones acerca de las posibles incompatibilidades de la obsolescencia programada con el sistema de defensa de los consumidores*, in *Actualidad Civil*, 2015, 6, 40 ss.

[26] In tal senso, v. D. RAES, *L'obsolescence programmée à l'épreuve de l'obligation d'information du vendeur, de la notion de conformité et de la garantie des vices cachés*, in *Liber amicorum François Glansdorff et Pierre Legros,*Bruxelles, 2013, 272 ss.; A. HAMANN, *Obsolescence programmée: le droit en panne*?, in *D.C.C.R.*, 2014, 68-69.

[27] Gli interpreti sia teorici sia pratici hanno offerto una nozione ampia di difetto materiale, ai sensi del § 434 del BGB, tale da includere anche quello derivante da condizioni di produzione che si traducono in una carenza di determinate qualità ambientali od ecologiche del bene: C. MELLER HANNICH, E. KRAUSBECK, *Sustainability, the Circular Economy and Consumer Law in Germany*, in *EuCML*, 2020, 4, 170; T. BRÖNNEKE, *Premature Obsolescence: Suggestions for Legislative Counter-measures in German and European Sales & Consumer Law*, in *JEEPL*, 2017, 14, 365. Sul tema, cfr. *amplius* J. CROON GESTEFELD, *Die nachhaltige Beschaffenheit der Kaufsache*, in *NJW*, 2022, 497 ss., ed ivi anche gli opportuni riferimenti giurisprudenziali.

per i prodotti, fra cui quelli per la valutazione delle potenzialità di un miglioramento degli aspetti ambientali, in cui è, in particolare, incluso quello consistente nella «estensione della durata espressa in termini di: durata minima garantita, tempo minimo per la disponibilità di parti di ricambio, modularità, possibilità di upgrading, riparabilità».

Così, il Reg. n. 666/2013 dell'8 luglio 2013 recante modalità di applicazione della suddetta direttiva 2009/125/CE in merito alle specifiche per la progettazione ecocompatibile degli aspirapolvere, prevedeva (Allegato I, 1.b) che «il tubo, se esistente, deve avere una buona durabilità in modo che sia ancora utilizzabile dopo 40000 oscillazioni sotto sforzo» e che «la durata di vita del motore deve essere pari o superiore a 500 ore».

Così, il Reg. n. 2017/745 del 5 aprile 2017, relativo ai dispositivi medici, impone al fabbricante di un dispositivo impiantabile di fornire «informazioni sulla vita utile attesa del dispositivo e su ogni follow-up necessario» (art. 18, § 1, lett. *c*).

Così, la Direttiva n. 2018/851/UE del 30 maggio 2018, che ha modificato la Direttiva 2008/98/CE relativa ai rifiuti, ed in particolare l'art. 9, impone agli Stati membri di evitare la produzione di rifiuti attraverso una serie di misure, fra cui quella consistente nell'incoraggiare «la progettazione, la fabbricazione e l'uso di prodotti efficienti sotto il profilo delle risorse, durevoli (anche in termini di durata di vita e di assenza di obsolescenza programmata), riparabili, riutilizzabili e aggiornabili».

Così, da quando è entrato in vigore il Reg. n. 2021/341/UE, i fabbricanti, gli importatori e i mandatari di elettrodomestici (ad es. apparecchi di refrigerazione, lavastoviglie per uso domestico o lavatrici per uso domestico) sono tenuti a mettere a disposizione dei riparatori professionisti almeno i seguenti pezzi di ricambio: alimentatore interno, attacchi per la connessione di apparecchi esterni (cavo, antenna, USB, DVD e Blu-Ray), condensatori superiori a 400 microfarad, pile e accumulatori, modulo DVD/Blu-Ray, se del caso, e modulo HD/SSD, se del caso, per un periodo minimo di sette anni dopo l'immissione sul mercato dell'ultima unità del modello.

4. La sostenibilità del mercato dei consumi nella Direttiva n. 2019/771/UE.

Come accennato, a distanza di vent'anni dalla emanazione della Direttiva n. 1999/44/CE, il legislatore europeo è nuovamente intervenuto in materia di contratti di vendita mobiliare conclusi fra un professionista e un consumatore, emanando le due Direttive 'gemelle' 20 maggio 2019 nn. 770/UE e 771/UE, che dovrebbero concorrere, integrandosi a vicenda (v. *considerando* nn. 20, 21 e 22 direttiva 2019/770/UE; *considerando* nn. 13, 14, 15 e 16 direttiva 2019/771/UE), a disciplinare «determinati aspetti», rispettivamente, dei contratti di vendita di beni mobili materiali, inclusi quelli con elementi digitali, e dei contratti di fornitura di contenuti o servizi digitali.

In termini generali, si può convenire sul giudizio espresso da molti giuristi europei, secondo cui l'approccio al tema della sostenibilità ambientale che emerge dall'analisi del testo di queste due direttive appare molto timido[28].

Se, infatti, da un lato, viene dichiarato espressamente l'obiettivo consistente nel raggiungere «modelli di consumo più sostenibili e un'economia circolare» (v. *considerando* n. 32) e viene a tal fine introdotto il nuovo elemento della «durabilità»[29], di cui viene data la definizione («la capacità dei beni di mantenere le loro funzioni e prestazioni richieste attraverso un uso normale»: art. 2, n. 13) e che diventa requisito oggettivo (di valutazione della) conformità al contratto del bene (art. 7, § 1, lett. *d*), nonché possibile oggetto di una garanzia commerciale (v. art. 17, § 1), dall'altro lato: *(i)* non viene imposto agli Stati membri di prevedere che sul professionista o sul produttore gravi l'obbligo di fornire specifiche informazioni sull'aspettativa di vita media dei prodotti che il consumatore può ragionevolmente attendersi, né di garantire la (o di informare sulla) disponibilità di pezzi di ricambio per un determinato periodo di tempo (che anzi viene espressamente escluso dalla portata della direttiva: v. *considerando* n. 33)[30]; *(ii)* analogamente all'impostazione seguita dalla Direttiva n. 1999/44/CE, è previsto, quale termine legale di durata della responsabilità del professionista-alienante, un termine di due anni da quando il difetto di conformità si manifesta, sia pure concedendo soltanto agli Stati membri la facoltà di derogarvi *in melius* (v. art. 10) e dando peraltro atto che «nella pratica tale periodo è considerato dagli operatori di mercato un lasso di tempo ragionevole» (sic) (*considerando* n. 41); *(iii)* è imposto agli Stati membri di prevedere una presunzione (relativa) di sussistenza del difetto di conformità al momento della consegna del bene per i difetti che si manifestano entro un termine circoscritto ad un arco temporale di un anno (sebbene superiore a quello previsto dalla Direttiva n. 1999/44/CE, che era di sei mesi), concedendo agli Stati membri soltanto la facoltà di derogarvi, prevedendo, comunque, al più, un termine di due anni per tale presunzione (v. art. 11 e *considerando* n. 45); *(iv)* non viene imposto alcun obbligo per gli Stati membri di prevedere sanzioni connesse al fenomeno dell'obsolescenza programmata.

Sul piano dei rimedi per difetto di conformità, poi, la Direttiva n. 2019/771/UE, pur declamando che «il fatto di consentire al consumatore di chiedere la riparazione dovrebbe incoraggiare un consumo sostenibile e contribuire a una maggiore durabilità dei prodotti» (v. *considerando* n. 48),

---

[28] Cfr. ad es. E. VAN GOOL, A. MICHEL, *The New Consumer Sales Directive 2019/771/UE and Sustainable Consumption: A Critical Analysis*, in *EuCML*, 2021, 4, 137, ove ulteriori riferimenti; J.M. CARVALHO, *The Premature Obsolescence of the New Deal for Consumers*, in *EuCML*, 2021, 3, 87; in termini analoghi, v. V. MAK-E. TERRYN, *Circular economy and consumer protection: the consumer as a citizen and the limits of empowerment through consumer law*, in *J. Cons. Policy*, 2020, 43, 1, 230.

[29] Il caso vuole che tale termine, nella lingua francese (*durabilité*), sia anche sinonimo di sostenibilità (*soutenabilité*). Per un ricco inventario di definizioni di 'durabilità' dei prodotti, rinvenibili nella letteratura, soprattutto economica, cfr. Commissione europea, *The Durability of Products*, Final Report, August 2015, 36 ss. Sul tema, cfr. G.F. SIMONINI, *Verso una nozione allargata di difetto di conformità: sarà rilevante anche la "durabilità" del bene?*, in *Danno e resp.*, 2019, 471 ss.

[30] Obblighi informativi circa gli aspetti relativi alla circolarità, quali la durabilità, la riparabilità o la riciclabilità, sono previsti da recenti provvedimenti normativi europei e in fase di attuazione (v. ad es. l'art. 6, § 1, lettera *b* della Direttiva n. 2005/29/CE, così come modificata Direttiva n. 2024/825, concernente la responsabilizzazione dei consumatori per la transizione verde mediante il miglioramento della tutela dalle pratiche sleali e dell'informazione, nonché il nuovo art. 23-*nonies* dell'allegato I, che include nelle pratiche commerciali sleali quella consistente nel «presentare come riparabile un bene che in realtà non lo è»).

sembrerebbe porre sullo stesso piano i rimedi conservativi (primari) della riparazione e della sostituzione del bene, la cui scelta spetterebbe al consumatore (v. art. 13: «ai fini del ripristino della conformità del bene, il consumatore può scegliere tra riparazione e sostituzione»)[31].

Sotto tale profilo, ed esaminando gli approdi cui è giunta la prassi giurisprudenziale formatasi nei diversi Stati membri, una *rara avis* è finora rappresentata da un'interessante decisione della Suprema Corte norvegese[32], che ha ritenuto legittimo e giustificato il rifiuto del venditore di sostituire un paio di stivali i cui tacchi si erano rotti dopo sei settimane dalla vendita conclusa dal consumatore (in considerazione dei relativi costi, di cui il venditore assumeva il carattere irragionevole), in quanto la riparazione era stata reputata dalla Corte norvegese il rimedio a più basso impatto ambientale, e ciò, anche perché in Norvegia non era dato registrare un mercato di scarpe di seconda mano in cui il bene avrebbe potuto essere ricollocato[33].

Più innovativa appare la disciplina relativa a quella categoria di beni (che possono formare oggetto di contratti che ricadono nell'ambito di applicazione della Direttiva n. 2019/771/UE) cui conviene il nome di 'beni con elementi digitali'[34], alludendosi con tale sintagma a tutti quei beni mobili materiali che incorporano o sono interconnessi con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni per le quali il bene è stato prodotto, indipendentemente dal fatto che tali contenuti o servizi digitali siano forniti dal venditore o da terzi (v. art. 2, n. 5, lett. *b*, art. 3, § 3 e *considerando* n. 14), e in particolare agli aggiornamenti, che – quali dati destinati ad integrarsi nell'ambiente digitale dei beni alienati, modificando o sostituendo altri dati già presenti al momento della consegna – influiscono sulla capacità di tale tipologia di beni di mantenere nel tempo tutte le caratteristiche e funzionalità (anche in termini di adattamento alle evoluzioni tecnologiche e di sicurezza) correlate allo scopo cui è normalmente destinato il loro utilizzo.

Con la Direttiva n. 2019/771/UE il legislatore europeo si è preoccupato di includere tali aggiornamenti nel novero dei requisiti oggettivi di conformità dei beni con elementi digitali e nell'oggetto della prestazione dell'alienante, nel

---

[31] In tal senso, v. ad es. E. Terryn, *A Right to Repair? Towards Sustainable Remedies in Consumer Law*, in *ERPL*, 2019/4, 855-856. Sul piano della legislazione europea, va, però, segnalata la previsione della legge slovena sulla tutela dei consumatori (art. 21.b ZVPot), che contempla una rigida gerarchia rimediale a tre livelli (P. Weingerl, *Sustainability, the Circular Economy and Consumer Law in Slovenia*, in *EuCML*, 2020, 3, 132), in base alla quale, in caso di difetto di conformità, il consumatore ha anzitutto diritto all'eliminazione del difetto (*id est*, riparazione del bene); soltanto se il difetto non viene eliminato entro il termine di 45 giorni dalla richiesta, il consumatore ha diritto alla sostituzione con beni identici, nuovi e privi di difetti; in via sussidiaria, infine, il consumatore può chiedere la riduzione del prezzo o la risoluzione del contratto.

[32] Høyesterett, 17.2.2006, menzionata da E. Maitre Ekern, C. Dalhammar, *Regulating Planned Obsolescence: A Review of Legal Approaches to Increase Product Durability and Reparability in Europe*, in *25 RECIEL*, 2016, 3, 390.

[33] Di tutt'altro avviso, è (ad esempio) la giurisprudenza olandese, pronunciatasi peraltro in casi relativi a beni tecnologici (District Court [Rechtbank] Amsterdam, 8 luglio 2016 e 18 aprile 2017, di cui ci riferiscono V. Mak-E. Lujinovic, *Towards a Circular Economy in EU Consumer Markets – Legal Possibilities and Legal Challenges and the Dutch Example*, in *EuCML*, 2019, 1, 9), secondo cui la protezione del consumatore, e dunque il suo diritto di scelta fra riparazione e sostituzione, assume rango prioritario rispetto ad altri interessi o valori.

[34] Su tale nozione, v. C. Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 2019, 520 ss.; A. De Franceschi, *La vendita di beni con elementi digitali*, Napoli, 2019, 50 ss. (ai quali si rinvia anche per la delimitazione delle rispettive aree di applicazione delle due Direttive 2019/770/UE e 2019/771/UE).

senso che l'omessa, incompleta o errata fornitura[35] degli aggiornamenti correttivi dell'elemento digitale necessari al fine di mantenere la conformità dei beni per un periodo di tempo che il consumatore può ragionevolmente aspettarsi (variabile in ragione della diversa tipologia e finalità dei beni e degli elementi digitali: v. *considerando* n. 31) è, di regola, valutata come difetto di conformità, anche se i beni risultavano conformi al momento della consegna del bene al consumatore[36].

È, infatti, previsto che, se il contratto di vendita prevede un unico atto di fornitura del contenuto digitale o del servizio digitale, il professionista ha l'obbligo di comunicare e fornire gli aggiornamenti (ivi compresi quelli di sicurezza), necessari al fine di mantenere la conformità di tali beni nel periodo di tempo che il consumatore può ragionevolmente aspettarsi, date la tipologia e la finalità dei beni e degli elementi digitali, e tenendo conto delle circostanze e della natura del contratto; se, invece, il contratto di vendita prevede una fornitura continuativa del contenuto digitale o del servizio digitale nell'arco di un periodo di tempo, il suddetto periodo di tempo è di due anni dalla consegna del bene con elementi digitali (pari a quello previsto per la durata della responsabilità del professionista per difetto di conformità del contenuto o del servizio digitale: v. art. 10, § 2), salvo che il contratto preveda una fornitura per un periodo ultra-biennale, nel qual caso l'obbligo (e la relativa responsabilità) del professionista permane nella maggior misura ad esso corrispondente (v. art. 7, § 3).

L'installazione è, tuttavia, configurata come un vero e proprio onere gravante sul consumatore, nel senso che, ove il professionista alienante abbia adeguatamente informato il consumatore circa la disponibilità dell'aggiornamento e le conseguenze della sua mancata installazione da parte del consumatore, la condotta consistente nella mancata installazione, da parte di quest'ultimo, degli aggiornamenti forniti entro un termine ragionevole (purché tale condotta non sia ascrivile a carenze delle istruzioni di installazione fornite al consumatore) assurge a causa di esclusione della responsabilità del professionista per ogni difetto di conformità che l'aggiornamento pertinente avrebbe prevenuto o evitato (v. art. 7, § 4 e *considerando* n. 30)[37].

5. La disciplina italiana di recepimento della Direttiva n. 2019/771/UE (D.lg. n. 170/2021) alla prova della sostenibilità.

Sul piano della sostenibilità, il legislatore italiano del recepimento della Direttiva n. 2019/771/UE, attuata con il D.lg. 4 novembre 2021, n. 170, che ha modificato le disposizioni contenute nel Capo I del Titolo III della Parte IV del

[35] La terminologia impiegata nel testo della Direttiva n. 2019/771/UE ('fornire'; 'fornitura'), ove riferita ai beni con elementi digitali (v. ad es. *considerando* nn. 13-16, 28, 30, 31, 37, 39, 41, 45), allude all'esecuzione di una prestazione più di *facere* che di *dare*.

[36] Atteso il carattere dinamico della prestazione dell'alienante di beni con elementi digitali, si è in proposito parlato di 'conformità continuativa' (F. Bertelli, *L'armonizzazione massima della direttiva 2019/771/Ue e le sorti del principio di maggiore tutela del consumatore*, in *Europa e dir. priv.*, 2019, 955).

[37] È stato opportunamente osservato che tale previsione rischia di incentivare comportamenti abusivi, da parte di venditori e produttori, fra i quali proprio quelli legati al fenomeno della obsolescenza programmata (A. De Franceschi, *La vendita di beni con elementi digitali*, cit., 120).

Codice del consumo, oggi intitolato «Della vendita di beni» (artt. 128/135-*septies* c. cons.)[38], non sembra aver mosso passi significativi o ulteriori rispetto a quelli compiuti dal legislatore europeo in sede di emanazione della medesima direttiva, che pur lasciava agli Stati membri ampi margini di manovra.

Se è vero, infatti, che – conformemente a quanto prescritto dalla fonte europea oggetto di recepimento (v. soprattutto artt. 2, n. 13 e 7, § 1, lett. *d*, nonché *considerando* n. 32 della Direttiva n. 2019/771/UE) – è stata introdotta la categoria della «durabilità» del bene (art. 128, 2° co., lett. *o*), che è quindi entrata ormai a pieno titolo nel lessico giuridico[39], ed è stata inclusa nel novero delle caratteristiche e delle qualità che il bene deve presentare per essere considerato oggettivamente conforme al contratto (art. 129, 3° co., lett. *d* c. cons.), occorre verificare e indagare se tale categoria sia, nella prospettiva della sostenibilità, foriera di obblighi ulteriori gravanti sul professionista alienante (sul punto, cfr. *amplius infra*, § 6).

Né è previsto dalla normativa di attuazione della Direttiva n. 2019/771/UE un obbligo legale di informazione circa l'aspettativa di vita media del prodotto in relazione alla tipologia o categoria merceologica di appartenenza ovvero circa la disponibilità di pezzi di ricambio, che pur il legislatore italiano avrebbe potuto introdurre (v. *considerando* nn. 20 e 33 Direttiva n. 2019/771/UE), a meno che non si tratti di beni con elementi digitali, in relazione ai quali incombe sul professionista alienante un obbligo di informazione avente ad oggetto gli aggiornamenti disponibili, anche di sicurezza (art. 130, 2° co., c. cons.), atti a mantenere nel corso del rapporto contrattuale – e anche oltre il periodo corrispondente al periodo di responsabilità del professionista, come si desume dal *considerando* n. 31 della Direttiva n. 2019/771/UE, che utilizza il parametro della ragionevole aspettativa del consumatore – la conformità del bene[40], e potranno essere, altresì, invocate le diverse disposizioni contenute negli artt. 48 e 49 c. cons., che – per effetto del recepimento dell'art. 4 della Direttiva n. 2019/2161/UE da parte del D.lg. n. 26/2023 – impongono al professionista di informare il consumatore in merito alla «funzionalità dei beni con elementi digitali, del contenuto digitale e dei servizi digitali, comprese le misure applicabili di protezione tecnica», nonché alla «compatibilità e interoperabilità

---

[38] Per un commento sistematico di tale disciplina, cfr. AA.VV., *La nuova disciplina della vendita mobiliare nel codice del consumo. La direttiva (UE) 2019/771 relativa ai contratti per la fornitura di cose mobili stipulati da professionisti con consumatori ed il suo recepimento nel diritto italiano (D.Lgs. 4 novembre 2021, n. 170)*, a cura di G. DE CRISTOFARO, Torino, 2022.

[39] F. ADDIS, *Spunti esegetici sugli aspetti dei contratti di vendita di beni regolati dalla nuova Direttiva (UE) 2019/771*, in *Scritti in onore di Antonio Flamini*, I, Napoli, 2020, 13; M. D'ONOFRIO, *Il difetto di durabilità del bene*, Napoli, 2023, 19 ss.

[40] Si tratta di vere e proprie obbligazioni gravanti sul professionista in forza della stipulazione del contratto con un consumatore-acquirente (G. PERFETTI, *Beni con elementi digitali e aggiornamenti nella novellata disciplina dei contratti di vendita B2C*, in AA.VV., *La nuova disciplina della vendita mobiliare nel codice del consumo*, cit., 274 e 275). Paradossalmente, è frequente che proprio la fornitura di aggiornamenti di contenuti digitali ingenerino anomalie in termini di riduzione di funzionalità del bene, sussumibili sotto il fenomeno dell'obsolescenza programmata, come accertato dall'autorità regolatoria di settore italiana nei casi *Apple* e *Samsung* (AGCM, 25 settembre 2018, PS11039, provv. n. 27365 e PS11009, provv. n. 27363), su cui v. A. DE FRANCESCHI, *Planned Obsolescence challenging the Effectiveness od Consumer Law and the Achievement of a Sustainable Economy*, in *EuCML*, 2018, 6, 217 ss.; A. GIANNACCARI, *Apple, obsolescenza tecnologica (programmata) e diritti dei consumatori*, in *Merc. conc. reg.*, 2019, 149 ss.; G. D'IPPOLITO, A. RE, *Obsolescenza programmata. L'AGCM sanziona Apple e Samsung*, in *Riv. dir. media*, 2019, 325 ss.; per ulteriori riferimenti, v. G. TOSCANO, *Nuove tecnologie e beni di consumo: il problema dell'obsolescenza programmata*, in *Actualidad Juridica Iberoamericana*, n. 16, febrero 2022, 381-382, nota 49.

pertinente dei beni con elementi digitali, del contenuto digitale e dei servizi digitali, di cui il professionista sia a conoscenza o di cui ci si può ragionevolmente attendere che sia venuto a conoscenza».

Anzi, la nuova disciplina della vendita di beni al consumatore – diversamente da quella previgente, nonché dalla disciplina della vendita di diritto comune (v. soprattutto art. 1491 c.c.) – consente di modulare la prestazione traslativa dovuta dal professionista alienante anche in senso sfavorevole al consumatore-acquirente, consacrando la validità ed efficacia di deroghe convenzionali ai requisiti oggettivi di conformità, che si traducono in patti di esclusione o limitazione della responsabilità del professionista, peraltro non soggetti alla disciplina dei limiti all'autonomia privata dettata dall'art. 135-*sexies* c. cons., purché il consumatore sia stato specificamente informato dal professionista della divergenza fra una delle caratteristiche del bene rispetto ai requisiti oggettivi di conformità e tale scostamento abbia formato oggetto di un espresso e separato accordo al momento della conclusione del contratto (v. art. 130, 4° co., c. cons., attuativo dell'art. 7, § 5, della Direttiva n. 2019/771/UE). Tale accordo, infatti, potrebbe *in thesi* riguardare la 'durabilità' del bene alienato, che peraltro non deve essere necessariamente usato (o, secondo il lessico impiegato della Direttiva n. 2019/771/UE, «di seconda mano»), né necessariamente 'analogico'[41].

L'aspettativa ingenerata nel consumatore sugli attributi del bene *sub specie* di durabilità risulta, invece, sicuramente tutelata nel contesto delle informazioni pubblicitarie o, più in generale, di dichiarazioni pubbliche rese dal produttore o da suoi rappresentanti, che vincolano chi le ha fatte secondo il paradigma della responsabilità c.d. contrattuale[42] (sempreché le dichiarazioni pubbliche non siano state corrette prima della conclusione del contratto con modalità identiche o simili a quelle con cui è stato veicolato il messaggio pubblicitario oggetto di correzione), atteso che la novella legislativa contempla, quale possibile e, aggiungiamo, preferenziale contenuto delle garanzie convenzionali offerte al consumatore, la «durabilità di determinati beni nell'arco di un determinato periodo di tempo» (art. 135-*quinquies*, 1° co., c. cons.).

Se, infine, si volge lo sguardo normativo alla disciplina delle azioni rappresentative a tutela degli interessi collettivi dei consumatori, prevista dal D.lg. n. 28/2023, attuativo dalla Direttiva n. 2020/1828/UE, la «riparazione» è espressamente contemplata soltanto quale uno dei possibili contenuti di un «provvedimento compensativo» adottato dall'autorità competente (v. nuovo art. 140-*ter*, lett. *h* c. cons.)[43].

---

[41] L'unico limite, sinora individuato in via interpretativa dalla dottrina con riferimento all'ipotesi di beni con elementi digitali, è l'esclusione, dal possibile oggetto di tale accordo, degli aggiornamenti (A. De Franceschi, *La vendita di beni con elementi digitali*, cit., 123).

[42] Cfr. F. Bertelli, *Le dichiarazioni pubbliche di sostenibilità nella fornitura di beni di consumo*, Giappichelli, Torino, 2022, 211, secondo cui al vincolo che sorge per effetto del solo perfezionamento della sequenza comunicativa «deve riconoscersi il valore di vera e propria fonte di una relazione obbligatoria». Sotto il vigore della disciplina precedente, v. ad es. E. Camilleri, *Qualità pubblicizzate e affidamento del consumatore. Spunti per il caso* Dieselgate*?*, in *Nuova giur. civ. comm.*, 2016, 711, secondo cui il messaggio pubblicitario finisce con il «caricare di ulteriori contenuti ciò che è contrattualmente dovuto in termini di qualità e prestazioni del bene».

[43] Il lemma 'riparazione' è da intendersi sia in senso ampio (come rimedio extracontrattuale volto a risarcire un pregiudizio del consumatore), sia in senso stretto (come rimedio contrattuale, volto a riparare un bene

6. Verso una nuova semantica della tutela ripristinatoria: la riparazione del bene come oggetto di un obbligo gravante sull'alienante.

Il quadro finora delineato, che si ferma soprattutto al dettato legale, deve fare, tuttavia, i conti con le potenzialità racchiuse nel principio (o valore) dello sviluppo sostenibile, che oggi assume carattere trasversale, sovranazionale e generale, tanto da scalzare l'esigenza di rafforzare la tutela individuale del consumatore[44].

Già all'indomani dell'entrata in vigore della Direttiva n. 2019/771/UE, alcuni giuristi europei avevano per vero proposto una nozione di 'durabilità' quale sinonimo di riparabilità o comunque quale termine idonea a ricomprenderla[45].

Oggi, il principio di sviluppo sostenibile assurge a vera e propria direttiva ermeneutica, che trova ulteriore linfa in fonti normative euro-unitarie successive alla Direttiva n. 2019/771/UE.

Così, a titolo meramente esemplificativo, nel Reg. UE n. 2020/852 (c.d. Regolamento Tassonomia) si sottolinea (v. art. 13, § 1, lett. *b* e *considerando* n. 28) che un'attività economica può contribuire alla transizione verso un'economia circolare aumentando, ad esempio, «la durabilità, la riparabilità, la possibilità di miglioramento e la riutilizzabilità dei prodotti, in particolare nelle attività di progettazione e di fabbricazione» e si prevede (v. art. 17) che sono contrarie al principio 'orizzontale' "non arrecare un danno significativo" all'economia circolare (*Do No Significant Harm*, in acronimo "DNSH": v. art. 5 Reg. UE n. 2021/241 e, più diffusamente, Reg. delegato UE n. 2023/2486) le attività economiche che, tenuto conto del ciclo di vita dei prodotti e dei servizi forniti, conducono a «inefficienze significative nell'uso dei materiali o nell'uso diretto o indiretto di risorse naturali quali le fonti energetiche non rinnovabili, le materie prime, le risorse idriche e il suolo, in una o più fasi del ciclo di vita dei prodotti, *anche in termini di durabilità, riparabilità, possibilità di miglioramento, riutilizzabilità o riciclabilità dei prodotti*» [corsivo nostro].

In fonti euro-unitarie ancora più recenti si legge, in termini più espliciti, che i principi dell'economia circolare europea sono i seguenti: «i. utilizzabilità; ii. riutilizzabilità; iii. *riparabilità*; iv. smontaggio; v. rifabbricazione o ricondizionamento; vi. riciclaggio; vii. reimmissione nel ciclo biologico; viii. altri potenziali modalità di ottimizzazione dell'uso del prodotto o del materiale» [corsivo nostro] (v. Allegato 2, Tabella 2 del Reg. delegato UE n. 2023/2772, che integra la direttiva 2013/34/UE sui principi di rendicontazione di sostenibilità). Alcuni di questi requisiti, fra cui quello della riparabilità, sono anche contemplati fra i requisiti di progettazione ecocompatibile per prodotti sostenibili dall'art. 5 del Reg. UE n. 2024/1781 (c.d. Regolamento ecodesign, ove è peraltro contenuta una nozione di «riparazione», per tale intendendosi

---

mobile non conforme al contratto): in tal senso, cfr. G. De Cristofaro, *Le «azioni rappresentative» di cui agli artt. 140*-ter *ss. c.cons.: ambito di applicazione, legittimazione ad agire e rapporti con la disciplina generale delle azioni di classe di cui agli artt. 840*-bis *ss. c.p.c.*, in *Nuove leggi civ. comm.*, 2024, 29.

[44] Sulla sostenibilità come 'terzo interesse' che (unitamente a quello del professionista e del consumatore) emerge dalla Direttiva n. 2019/771, v. ad es. F. Zoll, K.M. Południak-Gierz, W.K. Bańczyk, *Sustainable consumption and circular economy in the Directive 2019/771*, in Правоведение, 2020, 64/4,530-531.

[45] In questo senso, v. E. van Gool, A. Michel, *The New Consumer Sales Directive 2019/771 and Sustainable Consumption*, cit., 138; J. Croon-Gestefeld, *Die nachhaltige Beschaffenheit der Kaufsache*, cit., 501.

«una o più azioni effettuate per ripristinare il prodotto difettoso o il rifiuto a una condizione in cui consegue la finalità cui è destinato»: v. art. 2, § 1, n. 20).

Anche nell'ambito di analisi e studi internazionali sono stati individuati cinque modelli di business idonei a orientare i sistemi produttivi verso obiettivi di circolarità e sostenibilità, fra i quali è annoverato il modello "Estensione della vita del prodotto"[46], volto appunto ad estendere il ciclo di vita utile dei prodotti e a contrastare il fenomeno dell'obsolescenza programmata, per modo che venga estratto «quanto più valore possibile da ogni unità di risorsa consumata, sviluppando i prodotti in modo da farli durare a lungo e mettendo a disposizione aggiornamenti, servizi, parti di ricambio» e che si esplica secondo le seguenti modalità: (1) costruire per la lunga durata; (2) ricondizionare, ossia riportare i prodotti allo stato originale e rivenderli come nuovi; (3) ritirare/scambiare/ricomprare per rimettere sul mercato; (4) aggiornare; (5) "riempire di nuovo", ossia ripristinare una funzione che si esaurisce più rapidamente del prodotto stesso; (6) riparare, scegliendo come target clienti soddisfatti delle prestazioni del prodotto e non interessati a sostituzioni.

Di più. Da ultimo, è stata emanata la Direttiva n. 2024/1799 recante norme comuni che promuovono la riparazione dei beni (c.d. Direttiva sul *Right to Repair*, in acronimo "R2R")[47], che dovrà essere attuata dagli Stati membri entro il 31 luglio 2026 e il cui ambito di applicazione è oggettivamente delimitato sia dalla circostanza per cui il difetto del bene si deve verificare o manifestare al di fuori del periodo della responsabilità del venditore regolato dall'art. 10 della Direttiva n. 2019/771/UE sia dalla tipologia merceologica di beni, allo stato circoscritti a lavatrici per uso domestico, lavasciuga biancheria per uso domestico, lavastoviglie per uso domestico, apparecchi di refrigerazione, display elettronici, apparecchiature di saldatura, aspirapolvere, server e prodotti di archiviazione dati, telefoni cellulari, telefoni cordless e tablet, asciugabiancheria per uso domestico, beni che incorporano batterie per mezzi di trasporto leggeri. In particolare, la Direttiva 'R2R', che integra e in parte modifica la Direttiva n. 771/2019[48] e che, nel dichiarare di «perseguire gli obiettivi, nell'ambito del *Green Deal* europeo, di promuovere un consumo più sostenibile, un'economia circolare e la transizione verde», si propone di «promuovere la riparazione nel quadro della responsabilità del venditore» (v. *considerando* n. 5), e dunque di incentivare – sia nel contesto delle garanzie legali di conformità sia al di fuori di esso – la riparazione e il riutilizzo di beni di consumo non conformi[49], impone a carico del produttore (o di terzi da questi incaricati) un obbligo di riparazione a titolo gratuito o a un corrispettivo ragionevole (v. art. 5), salvo che la sua esecuzione non sia giuridicamente o praticamente impossibile (v. *considerando* n. 24).

---

[46] P. Lacy, J. Rutqvist, B. Lamonica, Circular Economy. *Dallo spreco al valore*, Milano, 2015, 63 ss., spec. 111.

[47] Per alcuni primi commenti, cfr. F. Bertelli, *Approvata la direttiva (UE) 2024/1799 sul diritto alla riparazione "R2R"*, in *Persona e Mercato*, 2024, 2, 682 ss.; M. Faccioli, *Economia circolare e sostenibilità ambientale nel diritto dei consumatori: prime note sulla dir. 2024/1799/UE recante norme comuni che promuovono la riparazione dei beni*, *ivi*, 2024, 3, 945 ss.; R. Carozza, *Riflessioni a margine della Direttiva 2024/1799/UE recante norme comuni che promuovono la riparazione del bene*, in *Rass. dir. civ.*, 2024, 1114 ss.

[48] Una delle novità consiste proprio nell'aver aggiunto alle caratteristiche e alle qualità che il bene deve presentare per essere considerato oggettivamente conforme al contratto quella della «riparabilità» (v. nuovo art. 7, § 1, lett. *d* della Direttiva n. 771/2019, così come modificato dall'art. 16 della Direttiva 'R2R'): G. De Cristofaro (cur.), *Vendite di beni mobili*, Pisa, 2025, 58.

[49] M. Faccioli, *Economia circolare e sostenibilità ambientale nel diritto dei consumatori*, cit., 947.

Con riguardo alla materia dei contratti di alienazione di beni mobili al consumatore, tutti questi indici normativi, letti anche alla luce dei principi oggi consacrati nell'art. 9, 3° co. e nell'art. 41, 2° e 3° co. della Costituzione[50], si traducono nella istituzione, sul piano ermeneutico, di una gerarchizzazione fra i due rimedi conservativi c.d. primari, nel senso che il consumatore al quale sia stato consegnato un bene non conforme è tenuto a richiedere il ripristino della conformità attraverso la modalità prioritaria della riparazione o, *ex converso*, il professionista deve rifiutare di soddisfare la richiesta di sostituzione del bene non conforme qualora la strada della riparazione sia ancora percorribile e non imponga costi sproporzionati in base ai criteri dettati dalla disciplina del codice del consumo51, ove per «costi sproporzionati» possono intendersi anche quelli relativi all'impatto ambientale e alle ricadute sull'ecosistema che l'esercizio del rimedio invocato dal consumatore potrebbe comportare[52].

Come si vede, si tratta, più che di un diritto (potestativo) spettante al consumatore (sebbene in tal senso sembri deporre anche il nuovo art. 13, § 2 *bis* della Direttiva n. 771/2019, introdotto dall'art. 16 della Direttiva n. 2024/1799, nonché l'art. 37 del Reg. n. 2023/988, che fa comunque salvi i diritti previsti dalle direttive nn. 2019/770 e 2019/771), di uno specifico obbligo (*ex lege*) gravante sul professionista[53], sia pure 'quiescente' e reso attuale (soltanto) dalla richiesta di ripristino della conformità proveniente dal consumatore, sempreché la sua esecuzione non sia impossibile, irragionevole o sproporzionata (*arg. ex* artt. 135-*bis* e 135-*ter* c. cons.)[54].

Del resto, se così non fosse, il consumatore-acquirente sarebbe spesso incentivato ad orientare la scelta verso la sostituzione rispetto alla riparazione, in considerazione della maggiore forza attrattiva che presenta la consegna di un bene nuovo sostitutivo di quello originario, sia perché i relativi modi e tempi di attuazione di tale rimedio appaiono generalmente più snelli e rapidi, sia soprattutto perché l'uso normale, anche prolungato, del bene originariamente consegnato in forza del contratto non comporta alcun costo aggiuntivo per il consumatore che abbia poi richiesto una sua sostituzione[55] (v. art. 135-*ter*, 4° co., c. cons., che recepisce sul punto l'orientamento della giurisprudenza europea formatasi sotto il vigore della previgente disciplina[56]). Tant'è vero che

---

[50] È da tempo pacifico che la normativa costituzionale esprime principi che reagiscono sull'interpretazione della normativa ordinaria (cfr. per tutti P. Perlingieri, *Norme costituzionali e rapporti di diritto civile*, ora in Id., *Scuole tendenze e metodi. Problemi di diritto civile*, Napoli, 1989, 115 ss.).

[51] Hanno proposto una lettura del paradigma della sostenibilità in funzione interpretativa e conformativa dei rimedi consumeristici F. Bertelli, *«Dichiarazioni pubbliche fatte dal o per conto del venditore», conformità oggettive ed economia circolare*, in Aa.Vv., *La nuova disciplina della vendita mobiliare nel codice del consumo*, cit., 242 ss.; Ead., *La riparazione impossibile e l'importanza del difetto*, in *Persona e Mercato*, 2023, 2, 272; E. Maitre-Ekern, C. Dalhammar, *Towards a hierarchy of consumption behaviour in the circular economy*, in *Maastricht J. Eur. Comp. Law*, 2019, Vol. 26, 419.

[52] In tal senso, v. R. Fadda, *La sostenibilità tra disciplina del contratto e tutela del consumatore*, Napoli, 2024, 124.

[53] R. Fadda, *La sostenibilità tra disciplina del contratto e tutela del consumatore*, cit., 126.

[54] Per l'individuazione dei presupposti e dei limiti di esercizio dei rimedi c.d. primari, ci permettiamo di rinviare *amplius* ad A. Maniaci, *Della vendita di beni*, in *Codice del consumo e norme collegate*, a cura di V. Cuffaro, A. Barba, A. Barenghi, Milano, 2023, 945 ss.

[55] Sul punto, v. D.M. Matera, *Difetto di conformità, gerarchia dei rimedi e sostenibilità ambientale nel nuovo art. 135*-bis *cod. cons. e nella Dir. 771/2019*, in *Riv. dir. priv.*, 2022, 463.

[56] C. Giust. CE, 17.4.2008, *Quelle*, C-404/06, in *Giur. it.*, 2008, 1085 ss. Giudica «[a] dir poco ambigua» la previsione normativa G. De Cristofaro, *Legislazione italiana e contratti dei consumatori nel 2022: l'anno della*

la Direttiva n. 2024/1799 si preoccupa – oltre che di arricchire il bagaglio informativo del consumatore su durata stimata dei prodotti, servizi di riparazione e indici di riparabilità – di attribuire vantaggi ulteriori derivanti dalla scelta del consumatore orientata ad ottenere la riparazione, estendendo il periodo di responsabilità del professionista e imponendo al professionista di fornire temporaneamente e gratuitamente al consumatore, nelle more dell'esecuzione dell'intervento di riparazione (che dovrebbe comunque avvenire entro un tempo ragionevole), un bene sostitutivo, eventualmente anche ricondizionato[57].

7. Conclusioni.

È emerso che, nel contesto della disciplina dei contratti di alienazione al consumatore di beni che presentino un difetto di conformità, il *favor* per la riparazione rispetto alla sostituzione è applicazione di una direttiva (prima che normativa) ermeneutica, di cui l'interprete si fa carico, nel rispetto del dato positivo, dei valori vigenti e delle *rationes* sottese alle fonti euro-unitarie che è chiamato ad applicare e che presuppongono o quantomeno reclamano – al di là e a prescindere dalla tutela del singolo consumatore e, più in generale, della categoria dei consumatori – la istituzione di un sistema di produzione di beni maggiormente duraturi e di un'economia sempre più circolare ed efficiente dal punto di vista eco-ambientale, i cui riflessi si possono apprezzare anche nella dimensione privatistica dei rimedi[58].

Ciò è destinato a valorizzare il ruolo attivo e propulsivo del giurista, il quale – come è stato già sottolineato da altri e ad altro proposito[59] – può pervenire a risultati molto più efficaci di quelli derivanti da una piana e, aggiungiamo, piatta lettura dei testi normativi in materia.

---

svolta. Verso un diritto "pubblico" dei (contratti dei) consumatori?, in *Nuove leggi civ. comm.*, 2022, 30, in relazione alle conseguenze derivanti da un uso 'anormale' del bene ricevuto in consegna dal consumatore.

[57] Se il legislatore europeo sia finora riuscito nel suo intento di promuovere e incentivare la riparazione come rimedio ripristinatorio della conformità è, poi, questione tutta da verificare (esprime molte perplessità al riguardo G. De Cristofaro, *Le incongruenze e le ipocrisie del diritto europeo* green *e il rimedio contrattuale della riparazione del bene non conforme al contratto di vendita: le innovazioni apportate alla disciplina UE delle vendite mobiliari* b-to-c *dalle direttive 2024/825/UE e 2024/1799/UE*, in *Nuove leggi civ. comm.*, 2025, 409 ss.).

[58] Cfr. F. Degl'Innocenti, *Verso un'autonomia contrattuale sostenibile. Profili regolatori europei delle catene globali del valore*, Pisa, 2024, 55-56, secondo la quale, in base al modello di economia circolare, «la prospettiva del *long termism* si lega soprattutto a strumenti correttivi del sistema produttivo e di consumo». In generale, sulla cultura della manutenzione, v. M. Di Sivo, D. Ladiana, *Cultura di manutenzione per l'economia circolare: principi e criteri per una lunga vita dei prodotti*, Pisa, 2021.

[59] G. Perlingieri, *Per una modernizzazione del diritto successorio tra legislatore e interprete. a duecento anni dal codice per lo Regno delle due Sicilie*, in *Foro nap.*, 2023, 8.

Mesquita LV, 'The contract as a tool for conflict management: procedural agreements and digital innovation' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252LVM

EJPLT
ISSN 2704-8012



The contract as a tool for conflict management: procedural agreements and digital innovation

Il contratto come strumento di gestione del conflitto: accordi procedurali e innovazione digitale

LURDES VARREGOSO MESQUITA
Professor at Polytechnic
Universidade do Porto and Universidade Portucalense
Researcher at the Instituto Jurídico Portucalense

Abstract

Dispute resolution is evolving from a judicial monopoly toward alternative methods increasingly shaped by digital technologies and artificial intelligence. The transition to Online Dispute Resolution, now irreversible, calls for tools that safeguard party autonomy and ensure procedural security. In this context, procedural agreements play a central role: they allow parties to define and control key aspects of the process, ensuring that individual preferences are respected. In the digital age, such agreements represent a crucial balance between innovation and self-determination.

La risoluzione delle controversie sta evolvendo dal monopolio giudiziale verso metodi alternativi, sempre più influenzati dalle tecnologie digitali e dall'intelligenza artificiale. La transizione verso l'Online Dispute Resolution, ormai irreversibile, richiede strumenti che tutelino l'autonomia delle parti e offrano sicurezza. In questo contesto, gli accordi procedurali assumono un ruolo centrale: permettono di definire e controllare il processo, garantendo il rispetto delle preferenze individuali. Nell'era digitale, tali accordi rappresentano un equilibrio tra innovazione e autodeterminazione.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: procedural law; procedural agreements; digital justice; online dispute resolution; digital age

Summary: 1. Introduction. – 2. Alternative and Online Dispute Resolution. – 2.1. The phenomenon of de-judicialisation and the emergence of ADR. – 2.2. Legislative milestones for ADR methods in Portugal and the European Union. – 2.3. Online Dispute Resolution: concept and scope. – 2.4. ODR models. – 3. Traditional procedural agreements. – 4. Procedural agreements in the digital era. – 4.1. ODR systems: from first to second generation. – 4.2. Procedural agreements: Enhancing security and trust in ODR. – 5. Conclusions.

1. Introduction.

The efficiency of the justice system is central to attracting and sustaining economic investment. According to some studies,[1] there is a clear and significant link between judicial efficiency and economic performance. Efficient courts reduce transaction costs and provide greater certainty in contract enforcement, which directly influences firms' willingness to engage in trade credit and investment. Where justice systems are slow or unpredictable, firms face higher risks and are less likely to extend credit or enter long-term business relationships. The authors[2] also show that judicial inefficiency disproportionately affects small and medium-sized enterprises, which rely more heavily on external credit and are less able to absorb enforcement costs. They further find evidence that inefficient courts can constrain market competition and limit overall economic growth by discouraging productive investments and innovation. Conversely, improvements in judicial efficiency enhance access to finance, foster business dynamism, and support a healthier economic environment. The study therefore concludes that strengthening judicial systems is not only a matter of legal fairness but also a crucial component of economic policy, with tangible effects on trade, credit, and growth.

Access to justice is also a factor which contributes to development,[3] although it has less impact on growth in richer countries. Access to justice increases growth by making the government more accountable and improving institutional quality. It leads to a lower share of public consumption in GDP, less public corruption, higher total productivity, better protection of property rights and better regulation of credit markets.

The development and modernisation of this sector are vital for creating a stable and predictable environment for business operations. High costs of accessing justice, procedural delays, and the complexity of legal processes

[1] I Aguiar-Díaz, E Mruk, MV Ruiz-Mallorquí, 'How judicial efficiency impacts trade credit and doubtful receivables' (2024) 57 European Journal of Law and Economics 63. <https://doi.org/10.1007/s10657-024-09793-0>.
[2] Ibid.
[3] A Deseau, A Levai, M Schmiegelow, 'Access to justice and economic development: Evidence from an international panel dataset' (2025) 172 European Economic Review 104947. <https://doi.org/10.1016/j.euroecorev.2024.104947>.

often deter investors, undermining confidence in the system and increasing perceived risks. By reducing uncertainty, minimising costs, and fostering trust, a modernised justice sector attracts both domestic and foreign investment, stimulates economic activity, and supports societal development. Ultimately, the efficiency of the justice system reflects a nation's commitment to upholding the rule of law and fostering sustainable economic growth.[4]

An inefficient justice system generates significant transaction costs, compelling economic actors to allocate additional resources either to the resolution of disputes or to the mitigation of legal uncertainty. The excessive duration of judicial proceedings delays the settlement of conflicts, undermines contractual performance, and jeopardises the stability of commercial relations. Such delays may further entail reputational harm and substantial financial losses. The adverse impact is particularly pronounced for small and medium-sized enterprises, as well as for foreign investors, who frequently lack both the financial capacity and the specialised local knowledge required to navigate complex procedural frameworks effectively.

Litigation costs are recognised as a human rights concern under Article 6(1) ECHR, which guarantees the right of access to a court. The European Court of Human Rights evaluates such costs through proportionality analysis, assessing whether financial barriers undermine effective access to justice. Key factors include excessive court fees, stamp duties, or security for costs, unreasonable methods of cost calculation, and disproportionate or unjustified claims by state authorities. The Court also scrutinises situations where non-pecuniary damages are offset by high costs or where a litigant's vulnerability is disregarded. These elements act as warning signs that litigation costs may breach the fair balance between individual rights and legitimate aims.[5]

This topic raises several considerations and questions, particularly regarding the gradual erosion of the judicial monopoly. As courts no longer hold exclusive control over the resolution of disputes concerning disposable rights, parties are increasingly empowered to take an active role in shaping how their conflicts are addressed. This shift has fostered the expansion of consensual dispute resolution mechanisms, grounded in the autonomy of the parties and expressed through procedural agreements.

The increasing adoption of alternative dispute resolution (ADR) mechanisms, such as mediation and arbitration, has further enhanced the efficiency of justice systems, particularly in the digital age. These mechanisms allow disputes to be resolved quickly and flexibly, addressing the rapid transformation of economic and legal landscapes. Digitalisation also plays a transformative role, streamlining court processes, reducing delays, and improving access to legal information, thereby strengthening the alignment between justice and economic investment.[6]

---

[4] The Report of the Permanent Observatory of Justice in Portugal underlines this. Boaventura de Sousa Santos, Conceição Gomes, *A Administração e Gestão da Justiça. Análise comparada das tendências de reforma* (Coord) (Centro de Estudos Sociais da Faculdade de Economia da Universidade de Coimbra 2001) 3-4.

[5] See S Djajić, 'Unlocking Justice: Access to Court and Litigation Costs Under the European Convention on Human Rights' (2025) 24 The Age of Human Rights Journal e9282 <https://doi.org/10.17561/tahrj.v24.9282>.

[6] Sousa Santos and Gomes, *Administração e Gestão da Justiça* (n 4) 153.

Procedural agreements offer an additional tool for enhancing efficiency and trust in the justice system. They empower parties to choose the most suitable method for resolving disputes – whether mediation or arbitration – and to define specific procedural aspects. This flexibility reduces the time and expense of dispute resolution while providing greater predictability and legal certainty, essential for fostering a competitive economic environment. However, procedural agreements must respect fundamental principles of procedural law, such as the right to be heard and equality of arms, ensuring both parties can present their case fairly. By balancing efficiency with procedural safeguards, these agreements contribute to modernising the justice system, strengthening trust among economic actors, and supporting sustainable and ethical growth.

Traditionally, procedural agreements can be used to define the rules of the proceedings, to prevent disputes, to choose a dispute resolution method through mediation or arbitration or a combination of these two mechanisms, or even to put an end to a dispute by agreement of the parties. Bringing the advantages of empowering parties to choose ADR methods into the digital age naturally extends to the evolution of procedural agreements. These agreements could enable parties to specify the online mechanisms they are willing to adopt (or reject) and outline the extent to which artificial intelligence (AI) may be used in the resolution process.

The digital age has reinforced and streamlined the use of these mechanisms, adapted to the new digital age. Let's look at some of the issues associated with the topic: What are ADRs and ODRs? How did the ODR movement begin? What impact has digital development had on this phenomenon? What examples do we have? What is their relationship with the will of the parties and procedural deals?

While briefly addressing what ADRs and ODRs are and tracing the origins of the ODR movement, the focus will shift to examining the transformative impact of digital developments on these mechanisms. The core of the discussion will explore the interplay between these mechanisms, party autonomy, and the use of procedural agreements, analysing how such agreements can shape the resolution process, particularly in the context of digital and online tools.

2. Alternative and Online Dispute Resolution.

2.1 The phenomenon of de-judicialisation and the emergence of ADR.

The landscape of dispute resolution has undergone a significant transformation in recent decades, marking a paradigm shift away from the traditional monopoly of judicial proceedings. This evolution reflects a growing recognition that courtroom litigation, while sometimes necessary, is not always the most effective or efficient way to resolve conflicts.

Increasingly, individuals, businesses, and even governments are turning to consensual and extrajudicial methods of dispute resolution, including mediation, arbitration, and negotiation, which offer parties greater control

over the process and outcomes of their disputes. They often provide faster, more cost-effective, and less adversarial ways to address conflicts compared to court litigation.

This shift is driven by several factors, including overburdened court systems, the high costs and lengthy timelines associated with litigation, and a growing awareness of the benefits of collaborative problem-solving. Moreover, many of these alternative methods allow for more creative and tailored solutions that can better address the underlying interests of the parties involved.

As a result, we are witnessing the end of the judicial system's monopoly on dispute resolution. While courts continue to play a crucial role in upholding the rule of law, they are increasingly viewed as one option among many in a diverse landscape of conflict resolution mechanisms.

2.2 Legislative milestones for ADR methods in Portugal and the European Union.

In Europe, influenced by developments in the United States, ADR began to emerge, prompting national and European legislators to create legal frameworks to regulate these procedures.[7] Over time, ADR has gained increasing recognition as an essential component of the legal landscape, offering efficient and cost-effective solutions for resolving disputes. In Portugal, the legal framework for ADR has evolved significantly. The foundation was laid with Law 31/86, which established the framework for voluntary arbitration in the country. Although not recent, this law marked an important step in formalising arbitration as an alternative to judicial proceedings. This framework was later modernised with Law 63/2011, which aligned portuguese arbitration practices with international standards, including the UNCITRAL Model Law. In addition, the establishment of Justice of the Peace Courts (Julgados de Paz) through Law 78/2001 provided a unique combination of mediation and simplified judicial proceedings, enhancing access to justice for citizens. Another milestone was Law 29/2013, known as the Mediation Law, which set out general principles for mediation in civil, commercial, family, and labor disputes. Furthermore, Law 144/2015 implemented the EU Directive on consumer ADR, creating a comprehensive framework for consumer dispute resolution entities and aligning Portugal with European standards.

At the European Union level, several legislative milestones have shaped the development of ADR mechanisms. Recommendation 98/257/EC established key principles for out-of-court bodies handling consumer disputes, laying the groundwork for consistent standards across member states. Directive 2008/52/EC, known as the Mediation Directive, aimed to facilitate access to ADR by encouraging the use of mediation in cross-border civil and commercial matters, thereby promoting amicable dispute resolution. Regulation (EU) 524/2013 created an online dispute resolution platform for consumer disputes, marking a significant step towards integrating ADR into the digital

[7] See S Barona Vilar, *Arbitraje y Justicia en el siglo XXI* (Civitas Ediciones 2007), 49-50.

sphere and providing a user-friendly tool for resolving disputes online. However, despite its initial promise, the platform has not achieved the expected level of success. As a result, the European Union is currently taking steps to improve the regulatory framework and explore more flexible and effective solutions to enhance online dispute resolution mechanisms[8]. Complementing these efforts, Directive 2013/11/EU, the Consumer ADR Directive, ensured that consumers could submit complaints against traders to ADR entities for all types of domestic and cross-border disputes involving contractual obligations.

Collectively, these legislative measures have been instrumental in promoting and regulating ADR methods, making them more accessible, reliable, and effective for both citizens and businesses across Europe. They underscore the growing importance of ADR in fostering a more efficient and inclusive justice system.

2.3. Online Dispute Resolution: concept and scope.

Online Dispute Resolution (ODR) initially gained prominence as a method to support consensual dispute resolution processes using electronic tools. These systems, predominantly offered by private companies, were developed to enhance client services and reduce reliance on litigation.[9] Examples of functionalities include online chat rooms and videoconferencing, designed to facilitate swift and cost-effective agreements. Some platforms go further, integrating AI and big data to propose solutions based on precedent cases, offering users tailored and data-driven resolutions.

From a business perspective, providing ODR mechanisms not only builds client loyalty and enhances market trust but also indirectly promotes access to justice and reduces the burden on judicial courts. Despite their economic motivations, these private-sector initiatives help mitigate resignation among users by offering accessible and efficient alternatives to traditional litigation. Consumer disputes have become a key area of application for ODR systems. As Fred Galves points out, "another benefit of ODR is its flexibility; various manifestations of ODR are possible. For example, the parties might agree to use all the procedures of the online system, but then have the final arbitration proceeding in person, as sort of a hybrid of ODR and traditional, in-person

[8] Regulation (EU) 524/2013, which established the European Online Dispute Resolution (ODR) platform, is currently undergoing a repeal process as per proposal COM(2023) 647 final, presented on 17 October 2023. The initiative aims to discontinue the ODR platform due to its limited uptake and overlap with other ADR mechanisms. The proposal also includes amendments to Regulations (EU) 2017/2394 and (EU) 2018/1724 to ensure coherence within the European legislative framework. This change reflects the European Commission's commitment to streamlining consumer protection mechanisms whilst maintaining effective channels for dispute resolution through existing national and cross-border facilities.

[9] eBay and Amazon pioneered the implementation of ODR in e-commerce, with eBay introducing its Resolution Center in the late 1990s and handling millions of cases annually. These early private ODR systems demonstrated the potential for automated and assisted dispute resolution in online marketplaces, serving as influential models for subsequent ODR developments in both private and public sectors. See AJ Schmitz, J Martinez, 'ODR and Innovation in the United States', in MSA Wahab, E Katsh, *Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution* (Eleven International Publishing 2021) 3-5; E Katsh, C Rule, 'What We Know and Need to Know about Online Dispute Resolution' (2016) 67 (2) South Carolina Law Review 329-344.

ADR".[10]

In recent years, a broader interpretation of ODR has emerged, encompassing systems that integrate multiple dispute resolution mechanisms – both consensual and adjudicative – within a single platform. These systems aim to address the evolving needs of the parties, ensuring that when consensual solutions are not possible, adjudicative mechanisms, such as judicial intervention, remain available. This broader definition includes all online dispute resolution systems, regardless of whether they are public or private.

While there is no universal consensus on the definition of ODR, it is widely understood as the application of digital technologies to prevent, manage, and resolve disputes through a variety of tools. Unlike traditional ADR, which is grounded in strict confidentiality, ODR systems often incorporate data collection from previous negotiations and rulings. This data is processed to enhance "intelligent" platforms and refine their capabilities over time.[11]

2.4 ODR models.

ODR emerged in the United States during the mid-1990s, driven by the exponential growth of e-commerce and the need for innovative mechanisms to address disputes arising in the digital environment. Early platforms not only laid the groundwork for modern ODR systems but also showcased a variety of approaches to resolving conflicts efficiently and cost-effectively. Three pioneering initiatives – Virtual Magistrate Project, Cybersettle, and Smartsettle – played a crucial role in shaping the field.[12]

The Virtual Magistrate Project (VMAG) was one of the earliest attempts to resolve internet-related disputes online. Its primary focus was on issues such as spam, intellectual property conflicts, and disputes between internet users and service providers. The process was designed to be simple and efficient. So, parties submitted their disputes via an online form, and a volunteer arbitrator, referred to as a virtual magistrate, reviewed the case and rendered a decision. The entire process was conducted through email, with a goal of resolving disputes within 72 hours. While VMAG was praised for its innovative approach, it faced significant challenges. Case volumes were low, jurisdictional ambiguities created enforcement difficulties, and the technological infrastructure of the time limited its functionality. Despite these obstacles, VMAG is considered a seminal project in ODR, offering valuable lessons for future systems.

---

[10] F Galves, *Virtual Justice as Reality: Making the Resolution of E-Commerce Disputes More Convenient, Legitimate, Efficient, and Secure* (University of Illinois Journal of Law, Technology & Policy 2009) 1-62.

[11] About the concept of ODR, see D Nunes, CM Paolinelli, 'Novos designs tecnológicos no sistema de resolução de conflitos: ODR, e-acesso à justiça e seus paradoxos no Brasil' (2021) 46 (314) Revista de Processo 4-5; K Mania, 'Online dispute resolution: The future of justice' (2015) 1 (1) International Comparative Jurisprudence 76-86.

[12] These models were analysed by taking into account: R Gellman, *A Brief History of the Virtual Magistrate Project: The Early Months* (National Center for Technology and Dispute Resolution, 1996); ML Tushman, K Herman, *Cybersettle (A)* (Harvard Business School Case 406-041, 2006); J Barnett, P Treleaven, 'Algorithmic Dispute Resolution – The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies' (2017) The Computer Journal; EM Thiessen, A Soberg, 'SmartSettle Described with the Montreal Taxonomy' (2003) 12 Group Decision and Negotiation 165-170.

Cybersettle, established in 1998, marked a shift towards automation in dispute resolution. Founded by lawyers in New York, it became the world's first automated settlement negotiation platform. Cybersettle introduced a blind bidding system where parties could submit up to three confidential offers. If the offers overlapped within a predefined range, the platform automatically calculated the settlement by splitting the difference. This system was particularly effective for resolving insurance claims, financial disputes, and commercial settlements. Cybersettle's innovative use of technology to streamline negotiations earned it significant acclaim, and its success demonstrated the potential of automation in reducing costs and delays. However, the platform was also criticised for its limited applicability to more complex disputes.

Smartsettle emerged as a more sophisticated platform, leveraging advanced algorithms to optimise agreements. Unlike Cybersettle, which focused on monetary disputes, Smartsettle was designed to handle multi-variable negotiations, making it suitable for complex cases such as commercial contracts, family disputes, and environmental agreements. Its system provided visual tools for analysing proposals and offered algorithm-generated settlement suggestions, enabling parties to explore creative solutions that might not have been apparent through traditional negotiation methods. Smartsettle was widely praised for its adaptability and potential to handle intricate disputes, but its reliance on advanced technology required a learning curve for users and limited its accessibility in its early years.

Each of these platforms contributed distinct innovations to the field of ODR. VMAG demonstrated the feasibility of resolving disputes entirely online, even if its practical implementation was constrained by the limitations of its time. Cybersettle's automated negotiation system showcased the efficiency of blind bidding for straightforward financial disputes, while Smartsettle's algorithmic approach provided a glimpse into the future of data-driven conflict resolution. These initiatives highlighted both the opportunities and challenges of integrating technology into dispute resolution, offering valuable insights that continue to influence the development of ODR systems today.

3. Traditional procedural agreements.

It is possible to empower parties in dispute resolution through procedural agreements – contracts that allow parties not only to select the dispute resolution mechanism they wish to pursue but also to define procedural aspects of that mechanism, provided these are legally permissible and fall within the scope of the parties' autonomy under the applicable procedural law. Let us consider some examples in abstract terms, without focusing on any specific legal system.

Procedural agreements may include pre-dispute resolution clauses, such as mandatory negotiation periods, tiered dispute resolution processes with defined timelines for each phase, and agreements to attempt mediation as a first step, followed by arbitration agreements. Another example is forum

selection agreements, which enable the parties to choose a specific court or jurisdiction, opt for private arbitration, or resort to judicial courts for certain types of disputes, always within the limits set by applicable procedural law.

These agreements may also stipulate mandatory waiting periods before initiating formal dispute resolution proceedings. Additionally, procedural agreements can address evidentiary matters, such as setting rules for expert testimony or determining the admissibility of certain types of evidence, such as written witness statements, which parties may agree to accept.

Confidentiality can also be safeguarded through agreements that protect sensitive information during dispute resolution or through non-disclosure agreements covering mediation discussions or settlement negotiations. Depending on the applicable procedural law, some of these aspects may already be ensured by existing legislation, but parties may further tailor their agreements to address their specific needs. For instance, procedural agreements may include waivers of class actions, enabling disputes to be resolved individually rather than through collective actions.

Other agreements might establish qualifications for decision-makers, specifying the expertise required of arbitrators or mediators, or even predetermining a panel of neutrals approved by both parties. Simplified procedures, such as summary judgments or early neutral evaluations, may also be agreed upon for specific types of disputes.

Finally, some agreements may allow exceptions for interim relief, enabling parties to seek urgent judicial intervention when necessary, or establish protocols for data sharing and preservation, particularly regarding the handling of electronic evidence.

These procedural agreements can be tailored to the parties' specific needs and the nature of their relationship. They may be incorporated into broader contracts or executed separately to create a more efficient and predictable framework for preventing and resolving potential disputes.

Although it is uncommon to find a general clause explicitly allowing the creation of procedural agreements, such a provision exists in Brazilian law, specifically in Article 190 of the Civil Procedure Code enacted in 2015. This article states: «Art. 190. When the proceedings concern rights that permit settlement, it is lawful for fully capable parties to stipulate changes to the procedure in order to adapt it to the specificities of the case and to agree on their procedural burdens, powers, rights, and duties, either before or during the proceedings».

Sole paragraph. The judge, either ex officio or upon request, shall review the validity of the agreements provided for in this article, refusing to apply them only in cases of nullity, abusive inclusion in an adhesion contract, or when one party is in a manifestly vulnerable situation.[13]

[13] For further discussion on this topic, see F Didier Jr, *Negócios jurídicos processuais atípicos no CPC-2015* (Editora JusPodivm, 2016).

4. Procedural agreements in the digital era.

4.1. ODR systems: from first to second generation.

The digital age has transformed dispute resolution, giving rise to online dispute resolution. First-generation ODR systems largely replicated existing ADR processes in a digital format. While offering some advantages in terms of accessibility and speed, they often lacked the flexibility and sophistication needed to address the unique challenges of online disputes. Second-generation ODR systems, however, utilize technology to fundamentally transform dispute resolution through the application of AI.[14] These systems incorporate functionalities such as automated negotiation systems, where AI-powered platforms handle simple disputes automatically by analysing settlement patterns to propose fair resolutions. They also include intelligent case management, where AI categorizes and prioritizes disputes, assigning cases to appropriate human mediators or arbitrators. Predictive analytics leverage algorithms to analyse past data and predict potential outcomes, helping parties make informed decisions. Natural language processing enables AI to review documents, identify key issues, and summarize complex legal texts. AI-driven chatbots and virtual assistants guide parties through the initial stages of the process, answering questions and assisting with documentation. Emotion recognition and sentiment analysis help mediators understand the emotional states of the parties and tailor their approach accordingly. Real-time language translation facilitates online dispute resolution in cross-border or multilingual disputes. Decision support systems provide human mediators with relevant case law, regulations, and precedents. Bias detection identifies potential biases in decision-making, promoting fairness. Lastly, outcome simulation tools help parties visualize different scenarios and potential consequences.

The potential of second-generation ODR systems introduces new challenges for parties in effectively utilising these mechanisms. As such, it is crucial that parties are afforded the opportunity to define the parameters of the mechanisms they wish to employ and establish the boundaries within which they consent to their use, particularly regarding the application of AI.

In this context, procedural agreements can serve as an essential tool, enabling parties to tailor the dispute resolution process to their specific needs and ensuring that their autonomy and preferences are respected. These agreements provide a framework for balancing the innovative capabilities of AI-driven systems with the safeguards necessary to maintain fairness and trust in the resolution process.

4.2 Procedural agreements: Enhancing security and trust in ODR.

When faced with an actual or potential dispute, parties often seek to take an active role in shaping how it will be resolved, selecting mechanisms that align with their objectives and facilitate compromise and consensual

[14] For more on second-generation ODR systems, see R Susskind, *Online Courts and the Future of Justice* (Oxford University Press 2019) 263-275.

outcomes. In the digital age, the availability of second-generation ODR systems, which combine traditional methods with advanced technologies such as AI, offers significant opportunities but also raises important considerations. Procedural agreements are essential in this context, as they enable parties to address potential concerns and tailor the ODR process to their specific needs, ensuring that it reflects their values and preferences while safeguarding the fairness and security of the proceedings.

Through procedural agreements, parties can determine in advance the most suitable ODR platform for their dispute, ensuring that the chosen forum is both secure and appropriate. This level of clarity fosters trust in the process and reduces uncertainties. Furthermore, these agreements allow parties to explicitly define the role of AI within the resolution process. They may decide whether to utilise AI-driven tools for tasks such as negotiation, data analysis, or decision support, thereby addressing concerns about transparency, control, and ethical considerations.

In addition, procedural agreements provide the flexibility to establish hybrid human-AI models that balance the efficiency of automation with the nuanced expertise of human professionals. For instance, AI could manage preliminary stages, such as organising claims or offering analytical insights, while human mediators or judges handle the more complex and sensitive aspects of the dispute. This integration of technology and human judgment ensures that the process remains both efficient and responsive to the unique characteristics of each case.

Moreover, procedural agreements empower parties to decide whether the resolution process should remain strictly consensual or, if necessary, escalate to an adjudicative or heterocompositive approach. By providing a structured framework for expressing their intentions, these agreements enhance the overall effectiveness of ODR systems while fostering a sense of security and control. They bridge the gap between technological innovation and the fundamental principles of justice, enabling parties to fully harness the potential of second-generation ODR systems while addressing challenges such as data protection, procedural transparency, and equitable access.

5. Conclusions.

The rapid evolution of technology, alongside a paradigm shift in the administration of justice towards a citizen-focused and participatory model, highlights the growing importance of selecting dispute resolution methods that align with the unique circumstances of each case and the preferences of the parties involved. In areas governed by available rights, individuals should have the ability to construct a resolution process that reflects their specific interests, if this is based on mutual agreement. This flexibility not only enhances access to justice but also fosters greater trust in the system.

The emergence of ODR introduces significant opportunities but also complex challenges, particularly in designing and managing mechanisms that are both effective and secure. Legal frameworks must strike a balance between embracing innovation and upholding essential procedural principles.

Within this context, parties should have the autonomy to not only accept or reject a proposed resolution method but also actively influence the structure and scope of the process to ensure it meets their needs. When opting for ODR, safeguarding the autonomy and security of the parties becomes paramount. This requires the integration of tools and frameworks that empower individuals to engage in the process while mitigating risks associated with advanced technologies, such as AI. These risks may include biases in automated decision-making, data privacy concerns, and the potential for reduced transparency.

Procedural agreements are uniquely positioned to address these issues, providing a mechanism for parties to establish clear boundaries, define acceptable uses of technology, and ensure that the resolution process remains fair and equitable. By proactively crafting procedural agreements, parties can anticipate and manage the challenges posed by technological advancements. These agreements enable a tailored approach that not only reflects the will of the parties but also ensures their protection in an increasingly digital world. As such, procedural agreements are not merely a tool for dispute resolution but a fundamental safeguard for preserving the balance between innovation, autonomy, and justice in the digital age.

Pellecchia E, 'GDPR and Blockchain Technologies: a complex relationship' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252EP

EJPLT
ISSN 2704-8012



GDPR and Blockchain technologies: a complex relationship

GDPR e tecnologie blockchain: una relazione complessa

ENZA PELLECCHIA
Full Professor of Private Law
University of Pisa

Abstract

The contribution starts from the consideration of the apparent radical incompatibility between blockchain technologies and personal data protection regulations and proposes a case-by-case assessment of the different technologies to focus on the actual critical issues. The solutions proposed by the EDPB guidelines and the reactions to them are illustrated.

Il contributo muove dalla considerazione della apparente radicale incompatibilità tra tecnologie blockchain e disciplina della protezione dei dati personali e propone una valutazione caso per caso delle differenti tecnologie per mettere a fuoco le effettive criticità. Vengono illustrate le soluzioni proposte dalle linee guida EDPB e le reazioni ad esse.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: blockchain; data protection; GDPR

Summary: 1. Apparent incompatibilities and case-by-case assessments. – 2. Blockchain technologies and personal data processing. – 3. Tensions between Blockchain and GDPR. – 4. The guidelines of the European Data Protection Board (EDPB). – 5. - Reactions to the guidelines of the European Data Protection Board (EDPB). – 6. The potential of blockchain technologies for the protection of personal data.

1. Apparent incompatibilities and case-by-case assessments.

Blockchain exploits the characteristics of a computer network of nodes and allows for the management and updating, in a unique and secure manner, of a register containing data and information (e.g. transactions) in an open, shared and distributed way without the need for a central control and verification entity, preserving the historical memory of transactions in an immutable way. The register is structured as a chain of blocks (accompanied by hashes linked together by referencing the hash of the previous block in the next one) containing the transactions, and consent is distributed across all nodes in the network.

All nodes can participate in the process of validating transactions to be included in the ledger, and each participant has a copy of each transaction, thus ensuring security and resilience against potential attacks. Each block is cryptographically linked to the previous one after being evaluated and subjected to a consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated in all copies of the ledger within the network, and any conflicts are automatically resolved using established rules.

At first glance, the General Data Protection Regulation and blockchain technologies appear to be two irreconcilable worlds: this irreconcilability could be summarised in the formula centralisation vs. distribution.[1]

The centralisation that inspires the GDPR is well represented by the principle of accountability, which expresses a concept of risk that is not limited to the stage of violation, but also extends to the previous stage: imposing on the data controller a risk management approach that involves the adoption of precautionary technical and organisational measures to protect data from external tampering or unauthorised disclosure. The principle of accountability is accompanied – as is well known – by the principles of privacy by design (from the design stage) and privacy by default (by default setting).

Distribution – as the most advanced frontier even compared to decentralisation – is instead the soul of blockchains. In centralised networks, network participants need a central authority to communicate with each other.

[1] M Pilkington, 'Blockchain Technology: Principles and Application', in F Xavier Olleros, M Zhegu (eds.), *Research Handbook on Digital Transformation* (Elgar 2016); ML Perugini, *Distributed Ledger Technologies e sistemi di blochchain. Digital currency, Smart contrats e altre applicazion*i (Giuffrè 2018).

Decentralised networks have multiple authorities that act as centralised "hubs" for a subgroup of participants, and participants can communicate with others through their hub. Distributed networks, which are more flexible than centralised and decentralised networks, allow each participant to communicate with others without the need for a centralised point: each full node in the network maintains a copy of the entire blockchain to ensure the validity of transactions.

Immutability, accessibility, sharing and transparency are strengths of blockchain that clash with the very philosophy that inspires personal data protection legislation. There have even been fears that this technology, by its very nature, may not be able to comply with European data protection rules, which in turn could stifle its development to the detriment of the European digital single market project.[2]

The potential friction between the way the law is structured and the way technologies operate is an interesting and much-debated topic. It has been observed that individuals' behaviour can be regulated by legal provisions, but also by the "architecture" of the physical or virtual environment in which they operate.[3] When the law conflicts with the hardware and software architecture that structures the environment in which a technology operates, several situations can arise. The technology can survive and be used, and violate the law. Or the law can prevail over the architecture, and the technology cannot be adopted or its benefits exploited. Or decisions are made on a case-by-case basis on costs and benefits, with confusing and unpredictable outcomes. Each of these outcomes is imperfect and leaves many with the belief that important social interests have been neglected or ignored. It is with this conflict in mind, that between architecture and law, that the question of the relationship between GDPR and blockchain must be understood.[4]

On closer inspection, a different perception of a complex relationship emerges, one that does not lend itself to clear-cut conclusions, especially given that blockchains are a "class" of technologies: there is no single version, as the term refers to many different forms of distributed databases that vary greatly in their technical and governance arrangements and in their structure.

The most important classification criteria are now fairly well known and relate to a few key distinctions: that between "permissionless" and "permissioned" blockchains, and that between public and private blockchains.

In the first subset – "permissionless" and "permissioned" blockchains – the main differences concern the identifiability of subjects, the method of node selection and the size of the network, the shared consensus mechanism, and the transparency of block content. In permissionless blockchains, access is not subject to restrictions, the network has no theoretical limits to its development, with consequences in terms of immutability given the extreme difficulty of obtaining the necessary consensus for any change; furthermore,

[2] F Faini, 'Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection' (2020) Resp. Civ. Prev. 305.
[3] L Lessig, *Code: And Other Laws Of Cyberspace* (Basic books 1999).
[4] U Tatar, Y Gokce, B Nussbaum, 'Law versus technology: Blockchain, GDPR, and tough tradeoffs' (2020) Computer law & security review 38.

each user can view the entire blockchain, bringing transparency to the highest possible level.

In permissioned blockchains, on the other hand, centralisation is greater because access is controlled through a pre-identification mechanism, with repercussions on the level of immutability (in abstract terms, it is easier to achieve the majority needed to make changes) and transparency (the complete view of the blockchain could be inhibited at certain nodes).

In the second subset – public and private blockchains – the emphasis is on IT infrastructure management. Public blockchains do not have a "top", as they are the result of the progressive addition of participants to the network. Private blockchains, on the other hand, can be traced back to an organiser who normally uses the characteristics of the blockchain to strengthen the security of traditional databases. Normally, public blockchains are also permissionless, but pre-identification upon entry could make them permissioned.[5]

These preliminary distinctions have implications for data protection, with the result that an assessment of the compatibility of distributed ledgers with the GDPR should preferably be based on a detailed case-by-case analysis that takes into account the specific technical design and governance structure: not all blockchains are compatible or incompatible with data protection regulations, as each use of the technology must be examined on the basis of its own characteristics.[6]

This article aims to highlight some critical issues but also some potential benefits of the relationship between blockchain and the GDPR, bearing in mind that not all blockchains are compatible or incompatible with data protection regulations, as each use of the technology must be examined on its own specific characteristics.

The European Data Protection Board also appears to be moving in this direction with its 2025 guidelines, which have not resolved all issues but – despite some criticism – provide guidance on harmonising personal data protection and blockchain technologies.

Not all issues are addressed in this paper, which is not intended to answer every possible question but rather to highlight the benefits of a case-by-case approach.

2. Blockchain technologies and personal data processing.

Article 4(2) of the GDPR provides a very broad definition of "processing",[7] according to which the addition of personal data to a distributed ledger, its continued storage and any further processing may be considered personal data processing.

---

[5] AM Gambino, C Bomprezzi, 'Blockchain e protezione dei dati personali' (2019) Dir. inf. 627.

[6] For this approach to the issue, see the study by European Parliamentary Research Service (EPRS), 'Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?' (2019) 4.

[7] Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

However, it is above all the broad concept of personal data – and its even broader interpretation – that brings blockchain operations within the scope of the GDPR (obviously when they involve personal data).

Article 4(1) defines "personal data" as any information relating to an identified or identifiable natural person ("data subject"); a natural person is considered identifiable if they can be identified, directly or indirectly, with particular reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

The Regulation adopts a binary perspective between personal data and non-personal data and only subjects the former to its scope. According to recital 26 of the GDPR, the Regulation does not apply to anonymous data.

In contrast to this binary legal perspective, reality operates on a spectrum between clearly personal data, clearly anonymous data (an uncontroversial example would be climate data from outer space that does not reveal information about those who collected it) and "a lot in between".[8]

The broad definition of personal data is generating much debate and has led some to observe that data protection law has become the "law of everything",[9] as in the near future all data could be personal data and therefore subject to GDPR requirements.[10] This is because technology is rapidly moving towards the perfect identifiability of information; datafication and advances in data analysis mean that everything contains information; and in increasingly "smart" environments, any information is likely to relate to a person by purpose or effect. [11] Anonymisation is increasingly difficult to achieve with the advancement of modern information technology and the indiscriminate availability of information.

On the other hand, pseudonymisation – understood as the processing of personal data in such a way that the personal data cannot be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person – does not remove pseudonymised data from the scope of the GDPR: according to the authoritative guidance of the Article 29 Working Party, pseudonymisation is not a method of anonymisation. It simply reduces the linkability of a set of data to the original identity of a data subject and is therefore a useful security measure, but pseudonymised data are still personal data, processed with a high degree of security in the perspective of Article 25 GDPR.[12]

In light of the taxonomy outlined by the GDPR with regard to data, interpreters' attention – in the specific context of blockchains – has focused primarily on so-called public keys, which serve as user identifiers, and on data

[8] N Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 1 Law, Innovation and Technology 40.
[9] L Edwards, *Law, Policy and the Internet* (Hart Publishing 2018) 84, according to whom 'what constitutes personal data is one of the central causes of doubt in the current data protection regime'.
[10] N Purtova (n 8) 40.
[11] E Pellecchia, 'Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR' (2020) Le nuove leggi civ. comm. 360.
[12] Art. 29 Working Party, Opinion 5/2014 on anonymisation techniques, adopted on 10 April 2014.

relating to transactions carried out via blockchain (so-called transactional data).[13]

In the context of blockchain, public keys serve as the identifiers mentioned in recital 30 of the GDPR. Blockchains are based on a two-step verification process with asymmetric encryption. Each user has a public key (a string of letters and numbers representing the user) and a private key (also a string of letters and numbers, which is best thought of as a password that should never be shared with others). Both keys have a mathematical relationship whereby the private key can decrypt data that has been encrypted using the public key.

Public keys therefore conceal the identity of the individual, unless they are linked to additional identifiers. A public key is therefore data that "can no longer be attributed to a specific data subject" unless it is combined with "additional information" such as a name, address or other identifying information, in line with the definition of pseudonymous data in Article 4(5) of the GDPR.[14] Identification, linkability and even inference can allow public keys to be linked to an identified or identifiable natural person, both on public and permissionless blockchains and on private and authorised blockchains alike.[15] Measures should therefore be taken to make it unlikely that the public key can be linked to an identified or identifiable natural person: the use of single-use public keys appears to be a good practice in this regard, but this is more easily achievable on private and authorised blockchains than on public and permissionless ones.[16]

Transactional data, on the other hand, refers to other categories of data that can be used on blockchains but are not public keys: this is data about the transaction itself, which could be a name, address or date of birth contained in the payload of a given transaction.

Transactional data constitutes personal data when it refers directly or indirectly to an identified or identifiable natural person.

Both public keys and transactional data can be used in plain text, encrypted form or hashed form when placed on the blockchain. When personal data is used in plain text, it undoubtedly remains personal data and is clearly subject to the GDPR. There is debate as to whether encryption or hashing are methods capable of transforming personal data into anonymous data. A cryptographic hash is a mathematical function that is fed with an input value that is transformed into a fixed-length output value. The same input always produces the same output; it is not possible to deduce the input of the hash from the output of the hash.

Hash functions are often used to remove personal identifiers (such as a name or customer number) and replace them with a pseudonym that is difficult to reverse. Whether hashed data always remains personal data for the purposes of the GDPR is a matter of debate. However, hashing will often generate pseudonymous, not anonymous, data: hash functions can reduce the linkability

[13] M Fink, 'Blockchains an Data Protection in the European Union' (2018) European Data Protection Law Review 24.
[14] M Berberich, M Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers' (2016) Eur. Data Prot. L. Rev. 422.
[15] A M Gambino, C Bomprezzi (n 5) 633.
[16] J Barcelo, 'User Privacy in the Public Bitcoin Blockchain' (2007) 6 Journal of Latex Class Files 3.

of a data set to the original identity of a data subject; as such, they are a useful security measure but not a method of anonymization.[17]

3. Tensions between Blockchain and GDPR.

As mentioned at the beginning, according to some interpretations, certain characteristics of blockchains would make them incompatible with the GDPR: among these, the impossibility of identifying a data controller, the impossibility of applying the rights of the data subject, the incompatibility with the right to erasure, and the conflict with the principle of data minimization.[18]

A more careful analysis reaches less drastic conclusions about the compatibility between the GDPR and blockchain, starting with the variety of blockchain technologies referred to in the previous pages. Permissioned/private blockchains have a significant degree of compatibility with the GDPR, while greater tensions undoubtedly exist with regard to permissionless/public blockchains.

The conflicts between the GDPR and blockchain technology are not all unsolvable: according to some, they can be managed by leveraging commonalities, developing new approaches and interpretations to shift the balance between the GDPR and blockchain technology, and adapting blockchain technology to the requirements of data protection law. In other words, the discrepancies should not manifest themselves as a zero-sum game in which technology survives at the expense of breaking the law or the law unilaterally dictates its terms on technology to the point of overriding it.[19]

For example, blockchain technology and the GDPR share the goal of strengthening data privacy and security. But they differ on how to achieve this goal. Transparency, increased individual control over data, data minimisation and encryption are fundamentals of blockchain technology that are broadly in line with some fundamental rules of the GDPR. The immutable and decentralised nature of the technology ensures the integrity and accuracy of data stored on the blockchain, greatly reducing the risk of it being illegally altered and distorted, since – unlike centralised archives – information is stored across a variety of systems. And the integrity and accuracy of personal data are among the fundamental aspects that, according to Article 25, must be taken into account when designing and developing a technology.

Furthermore, blockchain technology gives users a great deal of power and allows them to exercise individual control over the personal data they store in the blockchain database. This means that they can decide whether to share their personal data and can do so to the extent required by the respective

[17] M Fink (n 13) 22.

[18] For an initial in-depth analysis of the relationship between privacy and blockchain, V Devi, V Sabareshwaran, R Saravana Kumar, M Sivasankar, 'Privacy-Preserving Healthcare Architecture Using Blockchain', (2020) 9 IJCSMC, 116-120; S Sakho et al., 'Privacy Protection Issues in Blockchain Technology', (2019) 17 IJCSIS, 124-131; R De Le Cruz, 'Privacy Laws in the Blockchain Environment', (2019) Annals of Emerging Technologies in Computing, vol. 3, 34-44; G Alpa, 'Tecnologie e diritto privato', (2017) Rivista italiana per le scienze giuridiche; P De Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies', (2016) Journal of Peer Production, 1.

[19] U Tatar- Y Gokce-B Nussbaum, (n.4), 6.

transaction on the blockchain. In other words, they can limit the data shared to the minimum necessary to achieve the specific purpose.

The main critical issue concerns immutability, since once data is entered into the blockchain, it cannot be revoked or "forgotten": not because of centrally organised and enforced rules (which can be changed), but because of "architectural" rules based on the digitally constructed environment (at the hardware and software design stage). Any attempt to intervene on the stored data – even as a result of exercising the "right to be forgotten" – would alter the consistency of the entire blockchain, damaging its reliability.

It should nevertheless be noted that some of the critical issues identified in blockchain technology in relation to the GDPR are not attributable exclusively to the way in which its architecture is designed, but also to some extent to critical issues inherent in the GDPR itself: for example, the lack of a clear definition of erasure. In this regard, it has been argued that the European Court of Justice and national supervisory authorities could choose to interpret the GDPR in a way that accommodates the immutable nature of blockchain: deletion and immutability, it has been said, are irreconcilable only to the extent that deletion means something that is not possible in the context of blockchain architecture; there would instead be room for a definition of erasure that includes the minimisation of information that allows the identity of individuals to be traced.[20]

Some Scholars note that almost all blockchain incompatibilities can be resolved with a practical approach by the competent public authorities, recognising the peculiarities of the technology in question and giving priority to the commonalities between the EU regulation and blockchain. To this end, bringing the relevant stakeholders from public bodies and industry together around the same table is of the utmost importance in order to build a constructive dialogue aimed at achieving practical and balanced approaches.

Like many regulatory challenges, this stems from the fact that data regulation is a difficult issue. The GDPR is an important step forward in attempting to resolve this difficult issue, but as in most regulatory environments, a push-and-pull between regulators and the regulated, including emerging definitions (and redefinitions), has the potential to make a series of very difficult questions more tractable.[21]

4. The guidelines of the European Data Protection Board (EDPB).

During its April 2025 plenary, the European Data Protection Board (EDPB) has adopted guidelines on processing of personal data through blockchain technologies.[22]

As the use of blockchain technologies is expanding, the Board considers it important to help organisations using these technologies to comply with the GDPR.

[20] M Fink (n 13) 30 ff.; U Tatar, Y Gokce, B Nussbaum (n 4) 7.
[21] U Tatar, Y Gokce, B Nussbaum (n 4) 7.
[22] <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en>.

One of the most complex and debated issues regarding the application of the GDPR to blockchain technologies concerns the allocation of responsibilities amongst the various parties participating in the network. Decentralisation, a distinctive feature of many DLT architectures, cannot and must not be interpreted as an exemption from the obligations set out in the Regulation: on the contrary, the GDPR is based on the principle of accountability, requiring a clear identification of which of the parties involved determines the purposes and means of personal data processing.

The Guidelines refer to the previous EDPB guidelines on the concepts of controller, joint controller and processor (WP29, Version 2.0, 2021), reiterating that the distributed nature of a technology does not exempt from the obligation to identify legal roles and responsibilities. The technical complexity of a blockchain cannot result in a de facto removal of responsibility.

In the context of a blockchain, the entity that determines the purposes and essential means of processing (e.g. the type of data stored on the chain, the methods of access, the rules for participation in the network) must be classified as the data controller.

However, in many blockchain applications, these choices are the result of a joint decision between multiple parties (e.g. consortia, groups of validators), meaning that joint controllership under Article 26 of the GDPR is frequently established. Such joint controllership entails the need to define, in a transparent manner through agreements between the parties, their respective responsibilities and methods of cooperation, as well as to adequately inform data subjects of the main elements of such an agreement.

Where, on the other hand, a participant acts on behalf of the controller and in accordance with binding instructions, the role of data processor (Article 28 of the GDPR) applies, with a consequent obligation to draw up a contract in accordance with legal requirements.

The definition of governance plays a central role in correctly identifying the roles of the various actors.

In permissioned or private blockchains, the existence of a coordinating authority (e.g. a consortium or a promoting organisation) facilitates the distribution of responsibilities and the conclusion of agreements between participants. In this context, it is often possible to: specify precisely who determines the purposes and means of processing; determine which nodes have access to personal data and under what conditions; regulate the procedures for exercising data subjects' rights and managing requests. Conversely, in public (permissionless) blockchains, the absence of formal governance and a central organisation makes it more difficult to identify who has effective control over data processing. In such cases, the EDPB suggests considering the possibility of setting up consortia or ad hoc legal entities that can perform a coordinating and representative role, not least to ensure an effective channel for data subjects to exercise their rights.

In its guidelines, the EDPB explains how blockchains work, assessing the different possible architectures and their implications for the processing of personal data.

The guidelines highlight the importance of implementing technical and organisational measures at the earliest stages of the design of the processing.

The EDPB also clarifies that the roles and responsibilities of the different actors in a blockchain-related processing of personal data should be assessed during the design of the processing.

In addition, organisations should carry out a Data Protection Impact Assessment (DPIA) before processing personal data through blockchain technologies, where the processing is likely to result in a high risk to the rights and freedoms of individuals.

According to the Board, organisations should also ensure the highest protection of individuals' personal data during the processing so that they are not made accessible to an indefinite number of persons by default.

The guidelines provide examples of different techniques for data minimisation, as well as for handling and storing personal data. As a general rule, storing personal data in a blockchain should be avoided if this conflicts with data protection principles.

Finally, the Board highlights the importance of the rights of individuals especially regarding transparency, rectification and erasure of personal data.

One of the key points of the EDPB Guidelines 02/2025 is the recommendation that the adoption of blockchain technologies should be the result of an informed assessment, based on an analysis of necessity, proportionality and adequacy in relation to the purposes of the processing.

The principle of data protection by design and by default (Article 25 of the GDPR) requires that, from the design stage of the technological solution, all measures – both technical and organisational – be taken to minimise the exposure of personal data, limiting its dissemination and ensuring compliance with the principles of minimisation and purpose limitation.

The correct selection of the blockchain architecture is one of the most important decisions for compliance purposes. The guidelines emphasise the need to carefully assess the type of blockchain to be used based on:

- the characteristics of the intended processing;
- the nature and sensitivity of the data involved;
- the rights and freedoms of the data subjects potentially affected.

In addition to choosing the type of blockchain, the Guidelines encourage the adoption of Privacy-Enhancing Technologies (PETs) that limit the dissemination of personal information without compromising the functionality of the system. Among the most relevant solutions are:

- Zero-Knowledge Proofs (ZKPs): cryptographic techniques that allow the veracity of information to be demonstrated without revealing its content. These can be used, for example, to demonstrate a subject's suitability to carry out a transaction without exposing their identity or other sensitive information.
- Salted Hashing or secret keys, commitment schemes and advanced pseudonymisation techniques: methods that allow only digital fingerprints (hashes) or references to data to be stored in the blockchain, keeping the actual identification data off-chain and reducing the risk of exposure.
- Decentralised Identifiers (DID) and Verifiable Credentials: emerging approaches in the field of digital identity, which can help reconcile verification requirements with compliance with the principles of minimisation and control by the data subject.

The EDPB recommends accurately documenting the reasons that led to the selection of a particular architecture or technical solution, within the broader accountability required by the GDPR (Art. 5, para. 2 and Art. 24). In particular, it is suggested to specify: the reasons why blockchain is considered the most appropriate technology for the specific use case; the alternatives evaluated and the reasons why they were rejected; the risk mitigation measures envisaged.

This documentation will be essential both in the event of checks by the authorities and to ensure transparency towards data subjects.

In light of the guidance provided by the EDPB in the new Guidelines, organisations that use or intend to implement blockchain solutions are faced with the need to significantly update their personal data protection documentation. Far from being a mere formal requirement, this review is a strategic imperative to ensure compliance with the GDPR and mitigate the risks associated with the use of emerging technologies: corporate privacy documentation is, in fact, the backbone of the accountability required by the Regulation, serving as the tool through which the data controller can demonstrate that it has taken appropriate technical and organisational measures to ensure, and be able to prove, that the processing is carried out in accordance with the law (Article 5(2) of the GDPR).

5. Reactions to the guidelines of the European Data Protection Board (EDPB).

Reactions to the guidelines have been cautious and concerned.[23] There has been no real hostility, but some critical issues that still need to be resolved have been reported, noting that the guidelines risk undermining Europe's digital sovereignty by mischaracterising blockchain as a traditional IT service model rather than a foundational public infrastructure, especially in the case of permissionless blockchains. The EDPB's approach, while grounded in valid concerns, risks deterring innovation in Europe if not recalibrated. A more informed, differentiated, and decentralisation-aware regulatory stance will empower Europe to lead in responsible digital infrastructure.

The main concerns relate to the following issues: mischaracterisation of blockchain as controllable infrastructure; oversimplified application of gdpr roles; overly broad interpretation of personal data; infeasible erasure and rectification expectations; inadequate distinction between blockchain types.

In summary: criticisms are focused on the fact that the EDPB Guide lines treat blockchain as a technology akin to cloud computing, implying centralised control and deployment decisions. This conflation ignores the nature of permissionless blockchains (e.g., Bitcoin, Ethereum), which are already operational, autonomous infrastructures. The assumption that entities interacting with blockchains are automatically "controllers" overlooks the distinction between node operation and data determination. On permissionless networks, nodes typically do not determine processing

[23] <https://europeanblockchainassociation.org/2025/06/09/a-turning-point-for-blockchain-regulation-in-europe/>.

purposes or means; instead, they adhere to software protocols and act similarly to Internet routers or telecommunications relays. The guidelines regard metadata (e.g., public keys, hashes) as personal data, even in the absence of feasible re-identification. This presumption creates legal uncertainty for developers and users and could criminalise the use of privacy-preserving technologies that operate pseudonymously by design and in consequence, effectively driving decentralised innovation out of Europe. Imposing expectations like the right to erase on immutable infrastructures ignores both technical constraints and the public utility logic of blockchain. The focus should be on minimising personal data on-chain (data scarcity) and enabling privacy-preserving architectures, rather than forcing technical features that contradict the nature of permissionless blockchain. Finally, the guidelines fail to sufficiently distinguish between permissionless/public and permissioned/private blockchains.[24]

The guidelines adopted have generated wide and articulated reactions among institutional actors, market participants, civil society organisations and legal scholars. While there is broad recognition of the central role played by the EDPB in promoting consistency in the interpretation and application of the GDPR, the reception of its guidance reveals persistent tensions between legal certainty, technological development and regulatory flexibility.

From an institutional perspective, EU bodies and national data protection authorities generally regard the EDPB's guidelines as an essential instrument for ensuring the uniform application of data protection law across Member States. The guidelines are widely perceived as contributing to legal harmonisation and to the reduction of enforcement fragmentation, particularly in cross-border processing scenarios. This positive assessment is especially evident in areas where the EDPB has sought to clarify the interaction between the GDPR and other EU regulatory frameworks, such as competition law or digital market regulation. At the same time, institutional actors explicitly acknowledge the non-binding nature of the guidelines and the fact that their ultimate authority remains contingent upon judicial interpretation, most notably by the Court of Justice of the European Union.

The reaction of industry stakeholders is more ambivalent. On the one hand, business associations and sector-specific organisations frequently welcome the EDPB's efforts to provide interpretative guidance in areas characterised by legal uncertainty, such as international data transfers, the identification of controllers and processors, or the allocation of responsibility in complex processing chains. In this respect, the guidelines are valued for their potential to enhance predictability and compliance planning, particularly for operators engaged in transnational activities or operating in highly regulated sectors.

On the other hand, industry responses often express strong criticism where the EDPB's interpretations are perceived as excessively restrictive or insufficiently attuned to technological realities. This criticism is particularly pronounced in relation to guidelines addressing emerging technologies and data-management techniques, such as pseudonymisation, anonymisation, blockchain technologies and advanced tracking methods. In these contexts,

[24] <https://eudecentralisation.org/blockchain-and-gdpr/>.

stakeholders argue that the EDPB tends to adopt a precautionary approach that risks extending GDPR obligations beyond the text of the Regulation itself, thereby increasing compliance burdens and potentially discouraging innovation. Concerns are also raised regarding the timing of certain guidelines, especially where parallel judicial proceedings before the CJEU may significantly affect the underlying legal concepts.

Civil society organisations and consumer groups generally adopt a more favourable stance towards the EDPB's guidance, viewing it as a necessary counterweight to market-driven pressures and as a means of safeguarding the fundamental rights enshrined in the EU legal order. These actors often support the Board's strict interpretations, particularly where they reinforce data subject rights and accountability obligations. Nonetheless, even within this group, some concerns emerge regarding the accessibility and practical comprehensibility of the guidelines, especially for smaller organisations and individual data subjects.

Academic commentary tends to situate the reactions to the EDPB guidelines within a broader systemic analysis of EU data protection law. Scholars frequently emphasise the quasi-normative function of the guidelines, noting that, despite their formal non-binding status, they exert significant influence on supervisory practice and judicial reasoning. At the same time, academic debate highlights the structural tensions exposed by the guidelines, particularly the friction between legal principles rooted in centralised accountability models and technological architectures based on decentralisation, immutability or data replication. In this sense, divergent reactions to the EDPB's guidance are often interpreted not as a rejection of data protection objectives, but as a manifestation of deeper unresolved issues within the GDPR framework itself.

Overall, the reactions to the EDPB guidelines can be characterised as a combination of cautious endorsement and targeted criticism. While the legitimacy of the EDPB's coordinating role is rarely questioned, significant debate persists as to the appropriate scope and intensity of its interpretative intervention. This debate is especially salient in technologically complex domains, where the risk of regulatory over-reach must be balanced against the need to ensure effective and uniform protection of personal data within the European Union.

The reactions to the guidelines of the European Data Protection Board (EDPB) must be understood against the broader theoretical architecture of the GDPR, which combines a fundamental-rights-based approach with a risk-oriented and accountability-driven regulatory model. The EDPB's interpretative activity occupies a pivotal position within this architecture, functioning as a mechanism for ensuring consistency while simultaneously shaping the practical meaning of open-textured legal concepts.

From the perspective of EU institutional actors and national supervisory authorities, the guidelines are generally perceived as an essential instrument for realising the principle of consistency enshrined in Article 63 GDPR. In this sense, the EDPB's guidance is regarded as a functional extension of the GDPR's system of cooperative governance, aimed at preventing divergent national interpretations that could undermine both legal certainty and the uniform

protection of fundamental rights. This institutional reception reflects a conception of the GDPR as a composite regulatory framework, in which soft-law instruments play a structural role in ensuring the effectiveness of the Regulation.

At the same time, the institutional discourse surrounding the guidelines consistently emphasises their non-binding nature, thereby acknowledging the limits imposed by the principle of legality and by the CJEU's monopoly over authoritative interpretation of EU law. This tension illustrates a core theoretical feature of the GDPR: the reliance on flexible regulatory techniques that must nevertheless remain compatible with the requirements of democratic legitimacy and judicial oversight.

Industry reactions reveal a more ambivalent engagement with the EDPB's guidelines, which closely tracks the internal tensions of the GDPR itself. On the one hand, market actors tend to welcome guidance that clarifies the allocation of responsibilities, the conditions for lawful processing, or the application of GDPR provisions in complex processing ecosystems. From a theoretical standpoint, this support reflects the GDPR's accountability model, which presupposes that controllers and processors are able to assess risks and implement appropriate technical and organisational measures. Insofar as the guidelines reduce interpretative uncertainty, they facilitate the operationalisation of accountability and support compliance-oriented decision-making.

On the other hand, industry criticism becomes pronounced where the EDPB's guidance is perceived as transforming a risk-based framework into a quasi-categorical system of prohibitions. This criticism is particularly evident in relation to guidelines addressing emerging technologies or advanced data-management techniques, such as pseudonymisation, anonymisation or distributed ledger technologies. Here, stakeholders argue that the EDPB's precautionary approach risks undermining the GDPR's commitment to technological neutrality, by implicitly privileging certain technical architectures over others. From a theoretical perspective, such reactions highlight the difficulty of reconciling the GDPR's open-ended standards with the Board's tendency to stabilise interpretation through detailed guidance.

Civil society organisations and consumer representatives generally interpret the EDPB's guidelines through the lens of fundamental rights protection, which constitutes the normative core of the GDPR. These actors tend to support strict and rights-protective interpretations, particularly where the guidelines reinforce data subject rights or constrain expansive data-driven business practices. In theoretical terms, this reception reflects an understanding of the GDPR as a constitutional instrument of the EU legal order, designed to rebalance structural asymmetries between individuals and powerful data controllers. Nevertheless, even within this perspective, concerns occasionally arise regarding the accessibility and practical intelligibility of the guidelines, suggesting a tension between rights-maximisation and regulatory comprehensibility.

Academic commentary situates the reactions to the EDPB guidelines within a broader reflection on the normative function of soft law in EU data protection. Scholars frequently observe that, despite their formal non-binding

status, the guidelines exert a de facto normative influence on supervisory practice and judicial reasoning, thereby contributing to the progressive concretisation of GDPR principles. From this viewpoint, divergent reactions to the guidelines are not merely expressions of stakeholder interest, but symptoms of deeper structural tensions within the GDPR – most notably between decentralised technological architectures and a legal framework built around identifiable responsibility, controllability and ex post enforcement.

Overall, the reactions to the EDPB's guidelines reflect the inherent ambivalence of the GDPR itself: a Regulation that aspires to be technologically neutral yet rights-protective, flexible yet consistent, risk-based yet anchored in fundamental rights. The debate surrounding the scope and intensity of the EDPB's interpretative activity thus appears less as a contestation of the Board's legitimacy, and more as an ongoing negotiation over how GDPR theory should be translated into regulatory practice in an evolving technological environment.

With a view to collaboration rather than confrontation, a number of strategic options have been put forward: recognise the purpose and architecture of blockchain applications, particularly those aligned with permissionless public utility models (e.g. Bitcoin, Ethereum); regulation must be rooted in the governance intention behind the technology, not merely its technical components; shift from a provider-centric model of liability to a user-centric one; limit the classification of metadata (e.g., hashes, public keys) as personal data to contexts where re-identification is reasonably likely; recognise that blockchain operates more like a public utility than a private service; adapt governance models to reflect decentralised coordination, where participants operate based on mutual protocol rather than contractual arrangements.

6. The potential of blockchain technologies for personal data protection.

It has been argued that blockchain technologies could be a suitable tool for achieving some of the objectives of the GDPR. Indeed, blockchain technologies are a data governance tool that could support alternative forms of data management and distribution and offer advantages over other current solutions. Blockchains can be designed to enable data sharing without the need for a central intermediary, offer transparency on who has accessed the data, and blockchain-based smart contracts can automate data sharing, reducing transaction costs.[25]

These features can be invoked to support compatibility with some of the objectives of the GDPR, such as providing individuals with greater control over personal data that directly or indirectly concerns them.[26] The European

[25] M Berberich, M Steiner, op. cit., 425; see also C Wirth, CM Kolain, 'Privacy by BlockChain Design: A Blockhain-enabled GDPR-compliant Approach for Handling Personal Data', Reports of the European Society for Socially Embedded Technologies, 2018.

[26] AM Gambino, C Bomprezzi (n 5) 629, observe that blockchain could also curb indiscriminate data collection by large platforms such as Facebook or Amazon: encryption would guarantee selective access to data, in line with the principle of minimisation, as is the case with some blockchains mentioned by the authors, such as ShoCard and BCDiploma, which offer the advantage of maximum transparency on what data is processed and who has access to it, in line with the strengthening of data subjects' rights established by the GDPR.

Parliament, in its Resolution of 3 October 2018 on "Distributed ledger technologies and blockchain: building trust through disintermediation", explicitly considered blockchain to be a tool that strengthens citizens' autonomy by giving them the opportunity to control their own data and decide what to share in the ledger, as well as the ability to choose who can see that data.

A two-pronged approach can be developed to foster a virtuous relationship: designing blockchains that incorporate data protection techniques with a view to privacy by design and by default; and designing "dedicated" blockchains, i.e. those specifically designed to protect personal data.

Ultimately, blockchain technology can be redesigned and adapted to meet the requirements of the GDPR, albeit with some inherent compromises.[27] To this end, the blockchain industry and innovators should have a good understanding of the principles and objectives of the GDPR so that they can add new features and configurations to adapt the technology to the requirements of the GDPR, with a view to privacy by design.[28] To align blockchain technology with the needs of the right to be forgotten, blockchain innovators should propose a solution that allows personal data to be removed from blockchain ledgers. However, this solution should not be detrimental to the integrity of the chain. In other words, personal data should be removed from blockchain ledgers without breaking the consistency of the blockchain. This means that blockchain technology aligned with the right to be forgotten would require keeping the hash functions that link blocks intact, while allowing personal data to be removed from them. Chameleon hashes are being tested in this direction to create modifiable blockchains. It is not unusual for law and regulation to lead to changes in "architecture", and often important technological innovations arise from these changes to satisfy regulatory environments.[29] Another attempt to ensure GDPR compliance is to store personal data in off-chain archives. According to this solution, personal data must be detached from any other transaction data and placed in a separate off-chain repository. The authenticity of that personal data can be verified using corresponding hash functions stored in the blockchain network.

Protocols can be generated in such a way as to allow personal data stored in off-chain memory to be deleted without necessarily breaking the consistency of the chain. Deleting personal data stored off-chain will render the hash value useless. However, this solution reverses the advantages of storing data in a blockchain database in an immutable, tamper-proof, secure and transparent manner. With this solution, in order to comply with the GDPR, one may have to expose the blockchain to the vulnerabilities of off-chain storage, as well as potentially reinstate the need for trusted third parties, undermining one of the pillars on which distributed ledger technology is based.[30]

It is important that computer scientists, engineers and technologists take the public interest issues represented in the GDPR seriously, and that they are

[27] AM Gambino, C Bomprezzi (n 5) 631.
[28] L Moerel, 'Blockchain & Data Protection…and Why They Are Not on a Collision Course' (2019) European Review of Private Law 842.
[29] P De Filippi (n 18).
[30] U Tatar, Y Gokce, B Nussbaum (n 4) 7.

able to talk – both to regulators and to the public – about the advantages and disadvantages that each has in the context of blockchain. Emphasising the common values and objectives between the GDPR and blockchain will help to reduce the areas of controversy and conflict. Reinterpreting particular concepts in the GDPR will also offer flexibility and regulatory space.

Redesigning elements of the blockchain to create GDPR-compliant blockchains could be part of the answer, although it is likely to sacrifice some of the advantages that make blockchain such an attractive solution to many problems.[31]

[31] For this approach, see U Tatar, Y Gokce, B Nussbaum (n 4) 8.

Valle L, 'The role of the certification systems in the EU legal framework for sustainability goals, current state and future perspectives' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252LV

EJPLT
ISSN 2704-8012



The role of the certification systems in the EU legal framework for sustainability goals, current state and future perspectives

Il ruolo dei sistemi di certificazione nel quadro giuridico dell'UE per gli obiettivi di sostenibilità, situazione attuale e prospettive future

LAURA VALLE
Associate Professor of Private Law
Free University of Bozen-Bolzano

Abstract

Standards and certifications for sustainability are widely used by business operators to guide them in the introduction of sustainability practices and, through sustainability labels, to make their choices recognizable to competitors and consumers. The rules of standards and certifications supplement legal instruments for sustainability currently being developed at the European Union level. They are also particularly useful due to their potentially global nature, compared to statutory provisions, whose territorial applicability is limited. Within the European regulatory framework, EU Directive 2024/825 - directly aimed at regulating sustainability labels - has identified certain characteristics that certification systems must possess to avoid being classified as unfair commercial practices. Transparency, scientific justification of sustainability actions undertaken and reported, continuous monitoring and objective evaluation by a third-party organization of the activities carried out and the results achieved, and the importance (even if indirect) of measuring and measurable results. It follows that the Standards and Certifications currently in use, in order to fulfill their role in supporting the organization of business activities in a context driven by sustainability objectives, must undergo a process of improvement along the indicated lines.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Gli standard e le certificazioni di sostenibilità sono ampiamente utilizzati dagli operatori economici come guida per l'introduzione di pratiche sostenibili e, attraverso le etichette di sostenibilità, per rendere le loro scelte riconoscibili dai concorrenti e dai consumatori. Le norme relative agli standard e alle certificazioni integrano gli strumenti giuridici per la sostenibilità attualmente in fase di sviluppo a livello dell'Unione europea. Sono inoltre particolarmente utili per la loro natura potenzialmente globale, rispetto alle disposizioni di legge, la cui applicabilità territoriale è limitata. All'interno del quadro normativo europeo, la direttiva UE 2024/825 - volta direttamente a regolamentare le etichette di sostenibilità - ha individuato alcune caratteristiche che i sistemi di certificazione devono possedere per evitare di essere classificati come pratiche commerciali sleali. Trasparenza, giustificazione scientifica delle azioni di sostenibilità intraprese e riportate, monitoraggio continuo e valutazione obiettiva da parte di un'organizzazione terza delle attività svolte e dei risultati raggiunti, nonché importanza (anche se indiretta) della misurazione e dei risultati misurabili. Ne consegue che gli standard e le certificazioni attualmente in uso, al fine di adempiere al loro ruolo di supporto all'organizzazione delle attività aziendali in un contesto guidato da obiettivi di sostenibilità, devono essere sottoposti a un processo di miglioramento secondo le linee indicate.

Keywords: Certification; Standards; Sustainability; EU; Green

Summary: 1. Introduction. – 2. Certifications, standards and sustainability goals. – 3. Legal rules and private certifications. – 4. Certification schemes in the Recent EU Directives and EU Directive Proposals. – 5. EU Directive 2024/825, «Empowering Consumer for the Green Transition through better protection against unfair practices and through better information». – 6. The EU Proposal for a Directive on Green Claims. – 7. Certification schemes and the Corporate Sustainability Due Diligence Directive (CSDDD). – 8. The current state of standards and certification schemes under the EU Green Deal legal framework and the Clean Energy Development Plan. – 9. Conclusion.

1. Introduction.

Certification schemes have not attracted the wide attention of the legal literature so far, despite their consolidated role in several sectors of the contemporary economy,[1] and despite sometimes being expressly referred to in legal provisions.[2] This is the case in the fields of data processing and digital law,

[1] We can find scientific elaborations that connect certifications to the general theory of contract and to the legal system. About certifications as instruments to guarantee the protection of fundamental rights, L Maurin, *Contrat et Droits Fondamentaux* (LGDJ 2013) 364 ff. Certification systems and standards are indicated as instruments of a new sort of non-state protection of human rights by F Galgano, F Marrella, *Diritto e prassi del commercio internazionale* (Cedam 2010) 880-881. About contract law and certifications see also L Valle, *Il contratto e la realizzazione dei diritti della persona* (Giappichelli 2020) 305 ff.; J Yang, 'Contract Law Aspects of Sustainable Companies' Certification in the Global Value Chain' (2019) Eur. Rev. Contr. Law, 31 ff.
On ISO 26000 and SA 8000, see F Meco Tèbar, *ISO 26000 y IQNET SR10 Sistema de Gestión de Responsabilidad Social* and EE Taléns Visconti, 'SA8000: Cuestiones sociales y relativas al personal' in T. lo Blanch (ed.) *Responsabilidad Social y Sostenibilidad, El marco de actuación de la empresa* (Tirant 2023) 269 ff., 325 ff.

[2] A meeting between the representatives of the EU Commission and CEN (*Comité européen de Normalisation* – European Committee for Standardization) was held in June 2025 on key Regulations and Directives on

see for example Art. 42 of EU Reg. 2016/679 on the protection of natural persons with regard to the processing of personal data[3] and Art. 46 ff. of EU Reg. 2019/881 on cybersecurity certification schemes.[4] And now, in the field of sustainability law, see Recital 7 of EU Dir. 2024/825[5] which we will examine in this article.

One of the areas in which certification schemes currently play, and are going to play a role in the next future, is precisely that of the compliance with sustainability standards, both environmental and social.

Of particular current interest is examining how existing certifications operate within the framework of the emerging legal rules on sustainability goals. And – first of all – if the existing certification systems, and standards on which certifications are based, are in line with the rules on sustainability goals.

2. Certifications, standards and sustainability goals.

In the field of environmental law, re-known certification schemes were drafted well before the widespread interest in sustainability goals that characterize the current times, following the adoption of the UN Sustainability Development Goals (SDGs) and the Agenda 2030, agreed in 2015 and effective since 2016.

Those certification schemes are EMAS and Ecolabel established by EU public authorities in the '90s.[6]

EMAS was created by EU Regulation n. 1836/1993 as a voluntary tool that companies and other organizations can adopt to improve their environmental performances and to inform the public about the management of their environmental resources and issues. The purpose of EMAS was, since the

climate change and their interface with standardization. We can therefore ask ourselves whether things will change in the near future, towards an improvement in the use of ISO-CEN standards on climate change in the European legislative framework.

[3] That states that the recourse to a certification has the purpose to verify the compliance to the rules on data processing by the data controller or the data processor. Following art. 42.1, the certification organizations must be accredited by the competent supervisory authority or by the national organization of accreditation, in this last case in compliance with the standard ISO 17065/2012. D Poletti, C Causarano, 'Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione', in E. Tosi (ed.), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy* (Giuffré 2019) 369 ff.; 'Comment to Art. 42', in C. Kuner, L.A. Bygrave, C. Docksey (eds) *The EU General Data Protection Regulation (GDPR), A Commentary* (Oxford) 732 ff.

[4] Moreover, in the digital law field, the AI Act (EU Reg. 2024/1689) at art. 40 refers to standardization and harmonized standards. On standardisation and certification about Artificial Intelligence, see DE Harasimiuk, T Braun, *Regulating Artificial Intelligence* (1st edn, Routledge 2021) 95 ff.

[5] Recitals of EU directives or regulations are not themselves rules of law, nonetheless they have a strong importance for the interpretation of legislative provisions. On the role of *consideranda* or recitals, ECJ, 24.11.2005, C-136/04, and ECJ, 19.12.2019, C-418/18, that states that «the recitals of an EU act constitute important elements for the purpose of interpretation, which may clarify the intentions of the author of that act» and repeats, as was decided in 2005, that «however, the preamble to an EU act has no binding legal force and cannot be relied on as a ground either for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner that is clearly contrary to their wording». The EU Dir. 2024/825 amends previous directives, and for this reason its articles are very concise so that the *consideranda* (recitals) can play an important role in understanding the Directive's provisions. About the recitals and their content, M den Haijer, T van den Abeelen, A Maslyka, 'On the use and misuse of recitals in European Union Law', Amsterdam Law School Research Paper, No. 2019-31.

[6] We can think, in fact, that the concept of sustainable development is stated in the well-known Brundtland Report of 1987.

beginning, which of contributing to the achievement of the sustainable economic development.[7] This certification system is based on the standard ISO 14001:2004, and its communication to the public takes place through an Environmental Declaration that reports information and relevant data on the environmental impact of the organization. Organizations adhering to EMAS adopt a special label (logo)[8] and receive the registration on a special national list.[9]

Ecolabel is an EU trademark elaborated by CE Reg. n. 880/92 and is currently regulated by EU Reg. n. 66/2010, adopted to certify the environmental impact of products and services. This certification can be accessed on a voluntary basis by companies of all the EU Member States or companies from Norway, Iceland and Liechtenstein. The Ecolabel follows the standard ISO 14040 and, using a recognizable logo, gives to consumers the possibility to understand that the product is environmentally friendly throughout its life cycle.

Alongside these certification systems (EMAS and Ecolabel) regulated by EU law, private standards have made their first appearance in the field of environmental law at the international level.[10] In fact, private standards, that satisfy the need of the sector for detailed and technical rules, can have a global dimension. As observed, «over the past few decades, private or quasi-private international agencies and organizations have developed a vast variety of environmental standards, covering different areas of global production». They [the standards] could be developed by private and quasi-private actors, or created within the framework of international organizations. In some cases, environmental standards emerge from a collaboration through networks of private and public actors. «Such standards are often associated with certification and labelling schemes to attest the product or organization's compliance with the standards».[11]

The relationship between standards and certifications is of this kind: standards[12] provide the rules to follow when aiming at certain objectives, and

[7] EMAS II was regulated by EU Reg. 761/2001, later amended by EU Reg. 196/2006. EMAS III was regulated by EU Reg. 1221/2009 that repealed the previous EU Regulation.

[8] To be recognized as compliant to EMAS organizations need to pass a conformity evaluation by an accredited verifier, who validate the Environmental Declaration and its annual updates.

[9] The number of the registrations on this list is small compared to the number of ISO 14001 certifications accredited in Italy. In 2009 the number of accredited ISO 14001 certifications was about ten times more than the EMAS registration.

[10] E Orlando, 'Principles, Standards and Voluntary Commitments in International Environmental Law', in E. Techera, J. Lindley, K.N. Scott and A. Telesetsky (eds) *Routledge Handbook of International Environmental Law* (2nd ed., Routledge 2021) 23 ff., refers that standards related to environment and sustainability are very diverse among them in terms of actors and addressees, as well as in relation to their objectives and substantive contents.

[11] Orlando (n 10) 24.

[12] When, in particular, the so-called technical standards are mentioned, those standards are elaborated for the uniformation of the safety and quality characteristics of certain goods or services. The EU Dir. n. 98/34, that deals with information procedures in the field of technical standards and regulations, states that a standard is a technical specification approved by a recognized standardization body for repeated or continuous application, the compliance with which is not mandatory and is included among the following: international standard (ISO), European standard (EN) and national standard (UNI). The EU Dir. n. 98/34 has been modified by EU Reg. n. 1025/2012. Those standards are legally binding only if recalled by a law or a regulation, or recalled by a contract or the contract documentation (including pictures, advertising, etc.) of a certain producer that indicate to be compliant with them, or in the case in which they incorporate the state of the art. Cfr. Valle (n 1) 300, note 123. About ISO see *infra*, note 24, and the text in correspondence of the footnote.

certification systems serve to evaluate whether these standards have been met.[13] This is true, even if in the practice of market operators and in everyday language standards and certifications are often referred to together, as if they were a single tool. To give an example with one standard among the others, it is common to mention the "certification ISO 14001" to indicate a certification process according to the ISO 14001 standard.

Certifications provide, then, an assessment of conformity about products, services and processes, which ensures that standards have been met. Indeed, not any set of standards is subject to a certification assessment. When this happens, these types of standards have been called «*norms sans certification*»,[14] while in the other case, where compliance with the standards is subject to an assessment, an audit, these standards have been called «*norms de certification*».[15]

Audits – which assess compliance with the "rules" - can be first, second or third party. The first-party audit is set up to be based on internal monitoring by the company itself, possibly with the help of an advisor. The second-party audit is performed by the client of the supplier, or by a contracted organization on behalf of the customer. The third-party audit is based on checks carried out by an independent certification body that, at the end of the procedure, if the outcome is positive, issues a certificate of conformity. The final documentation of the certification is then "the certificate".[16]

Nonetheless, not all standards are technical standards. Sometimes we have also standards coming from sectorial agreements or non-profit organizations (see, for an example, the standards elaborated by the foundation Fair Wear in the sector of clothing production, on which here further), that do not have this characteristic of uniformation, so that the use of the word standards in these last examples has a more general meaning. At the same time, as we will mention in the text, not all standards are subject to a certification. See for example the conditions and standards elaborated by the foundation Fair Wear, that are not subject to a certification; companies become members of the foundation and are not, as such, obliged to comply to all the conditions, but they commit to improve and must improve their working conditions in the production of clothing (which is the goal of the Fair Wear standards).

[13] Certification systems are programs offered on the market that certify/assure the conformity to a standard, that is a set of rules (for example technical rules) approved by a certain organization (usually a private organization, such as a non-profit organization, like for example the International Organization for Standardization, ISO, but not only, see *infra*, note 24). Certification systems are based on a contract relationship, and are based on the assessment by a third-party when impartiality of control is wanted/required. This characteristic – as we will see further in the text – has not always been an intrinsic character of a certification, but – as we will see in this article – the EU legislation is stressing the third-party control as a characteristic of a certification.

See EU Reg. n. 765/2008 that regulate the control over third-party certifications and the accreditation of the bodies responsible for certifications (art. 1: «this chapter shall apply to accreditation, used on a compulsory or voluntary basis, relating to conformity assessment, whether that assessment is compulsory or not, and irrespective of the legal status of the body performing the accreditation»). The impartial assessment in a certification system is assured by organizations which expertise and impartiality has been ascertain by an entity embodied by the national government, that in Italy is Accredia.

[14] An example of this kind of standards is the ISO 26000 (see also the following note), not thought to be subject to a certification, but to be chosen as a voluntary standard. That even if, in the reality, there are organizations offering services of independent evaluation on the company positioning on the basis of this standard, even if a certification process is missing.

[15] L Maurin (n 1) 364 ff., recalls as «*normes sans certification*» the system ISO 26000:2010 and the principles of the Global Reporting Initiative (GRI), that are standards for company reporting and, as «*normes de certification*», the standards SA 8000 on social issues and the ISO 14001 in the environmental field.

[16] See also Y Shen, M Faure, 'Private standardization for sustainability', in M. Santos Silva, A. Nicolussi, C. Wendehorst, P.S. Coderch, M. Clèment, F. Zoll (eds.) *Routledge Handbook of Private Law and Sustainability* (Routledge 2024) 450.

Only a certification that follows a third-party audit procedure is reputed to be trustworthy. The accreditation system for the organizations carrying out certification activities is regulated by EU Reg. 765/2008.[17] At the international level, accreditation is based on the international standard ISO/IEC 17011, which specifies the requirements for organizations that accredit conformity assessment bodies. The organization designated by the Italian government for accreditation in Italy is Accredia in both cases, in accordance with European regulations and international standards.

If we consider the wider area of "business and human rights",[18] here operate – at the international level – private standards known as Voluntary Sustainable Standards (VSS). As it was said, they «emerged to constrain the impact of business on human rights».[19] In particular, they can require products to meet specific economic, social and environmental sustainability metrics. They can refer to products quality or attributes, or to production and processing methods, as well as transportation.[20] The use of the acronym VSS has become consolidated, which helps us understand how voluntary sustainable standards have become commonly used.

The Voluntary Sustainable Standards emerged in the 1990s to discipline the production supply chain in response to a perceived failure of public governance to rule the field,[21] and in fact it was said that «VSS aim to provide more robust support for human rights than that offered by the state».[22]

By the 2000s certifications had become the "gold standard" of non-state regulation – as it was observed –, and the number of the Voluntary Sustainable Standards had grown by almost 400% between 1985 and 2016.[23]

---

[17] Art. 1 of the Reg. states that it «lays down rules on the organisation and operation of accreditation of conformity assessment bodies performing conformity assessment activities». See also *supra*, note 13.

[18] The expression "Business & Human Rights" (B&HR) marks a field of interest and research that deals with doing business respecting human rights. This field is connected to environmental law when we think that environmental issues have an influence on human rights, and a safe environment has been recognized as protected based on the right to life, art. 2 of European Convention of Human Rights. On this last point see also *infra*, par. 8.

[19] EA Benneth, *The efficacy of voluntary standards, sustainability certifications, and ethical labels*, in A. Marx, G. Van Calster, J. Wouters (eds.), *Research Handbook on Global Governance, Business and Human Rights* (Elgar publ. 2022) 177.

[20] The expression Voluntary Sustainable Standards (VSS) is used at the international level, also for example by UNCTAD. About VSS, see *infra*, note 23. Certifications and labels serve to signal the successful implementation of VSS, i.e. to signal that they have reached a certain grade of impact. This description comes from the UNCTAD website. See also the UNCTAD Report *Understanding Voluntary Sustainability Standards*, 2023.

[21] Benneth (n 19) 179.

[22] Benneth (n 19) 180.

[23] Benneth (n 19) 181. Voluntary Standards are a broad and non-homogeneous category, starting from the fact that they can interest more possible areas, among which are those of business and human rights and that of the voluntary environmental standards. Furthermore, they can be elaborated by many different actors, as public bodies, NGOs, sectorial business association or can be the result of sectorial agreements among companies. In the category of the Voluntary Standards are also included the rules of very general and important instruments as the UN "Global Compact" and the OECD "Guidelines for Multinational Enterprises" on which see *infra*, note 74 and 80). For a table that summarizes the main characteristics of the different types of standardization in relation to public and private environmental standards, see Shen, Faure (n 16) 451; and for a map of the "territory" of voluntary standards relevant to the business and human rights sector, see A Rasche, 'Voluntary standards for business and human rights: reviewing and categorizing the field, in A. Marx, G. Van Calster, J. Wouters (eds.) *Research Handbook on Global Governance, Business and Human Rights* (Edward Elgar 2021) 164 ff., 167.

From a more general perspective, private standards of general and diverse adoption had already come into use much earlier, if we consider the fact that the International Organization for Standardization (ISO), which is one of the first and most recognized international standard-setting bodies, was founded in 1946. Its aim was – and is – to develop international standards to facilitate the international trade in goods and services.[24] ISO has historically focused on product specifications and technical engineering standards, and only later entered into the environmental field, through the development of process-oriented and performance standards.[25]

In current times, we are witnessing a change compared to the experience of the '90s, that was characterized by the spread of the use of the VSS. Indeed, with the aim of pursuing sustainability goals, legal rules on business and human rights and environmental protection have begun to be developed and implemented, with particular attention to the sustainability of economic activities.

Legal regulations having the object of the realization of sustainability goals have grown to a considerable number, starting with the publication of the EU Green Deal at the end of 2019, within the framework of which we can find: the Corporate Sustainability Responsibility Directive (CSRD, Dir. 2022/2464), the Corporate Sustainability Due Diligence Directive (CSDDD, Dir. 2024/1760), the Taxonomy Regulation (Reg. 2020/851), the Sustainable Finance Disclosure Regulation (Reg. n. 2019/2088), the Eco-design Regulation (Reg. 2024/1781), the EU Directive "Empowering consumers towards the green transition" (Dir. 2024/825), to name the probably best known ones. Even prior to the EU legislative initiatives in the field, national laws had been published and enacted, in particular about the control of the supply chain: in France the Loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (2017), in Germany the Lieferkettengesetz[26] (2021), in Norway the Act relating to "Enterprises' transparency and work on fundamental human rights and decent working condition" (2021), in UK the English "Modern Slavery Act" (2015) and in the Netherland the "Dutch Child Labour Due Diligence Law" (2019). The Green Deal Plan was followed by the Clean Energy Development Plan published in autumn 2024,[27] more focused – in comparison to the previous one - on the development of circular production and clean energy, rather than on the control of the production's and supply chain. That means purely focused

[24] Orlando (n 10) 24. The International Organization for Standardization (ISO) is an independent, non-governmental organization composed of members of the national standards organizations of 161 States. The technique for adhering to ISO standards usually involves verifying compliance with the standards through a certification system. Cfr. L Valle, *Il contratto e la realizzazione dei diritti della persona*, cit., 300, note 123. For a short reference about ISO standards, F Marrella, 'Le organizzazioni non governative', in F. Galgano e F. Marrella, *Diritto e prassi del commercio internazionale* (Cedam 2010) 124. M Podrecca, M Sartor, *La qualità nelle organizzazioni, Certificazioni e standard internazionali* (McGrawHill 2025) 9, explain that in the '80s the growing globalization of commerce raised the need for shared standards at the international level to guarantee the quality of the production processes. Business enterprises in fact started to increasingly operate on a global scale, with supply chains spread across multiple countries and customers requiring consistent quality levels.

[25] Orlando (n 10) 24.

[26] The full name of the law is *Lieferkettensorgfaltspflichtengesetz.*

[27] For the transition from the EU Green Deal to the EU Clean Energy Development Plan see L Tenreira and others, *Unpacking the European Green Deal: redifining approaches, shifting methodologies,* Working Paper Law 2025/5, 5 ff.

on sustainable production systems from the environmental point of view, and less on the business and human rights implications that characterize the supply chain, first of all the implications concerning the protection of the human rights of workers. As we will see further, at par. 8, even if the so-called Omnibus Package of February 2025 has opened the way to a simplification of the obligations for the business enterprises under certain regulations (CSDDD, CSRD, the Taxonomy Regulation), several relevant legal acts in the field are in force, and others have recently been approved, or are in the process of being approved. At the same time, in the financial sector the need to comply with a series of sustainability requirements is stable or even increasing.[28]

3. Legal rules and private certifications.

The fact that legislation has finally assumed a significant role in the various aspects of the sustainability of economic activities and their communication, does not mean that private law rules – as standards and certifications – will no longer have a part in regulating the actions of economic operators towards sustainability objectives.[29]

Private certifications evaluation standards such as for example SA 8000, ISO 26000, B Impact Assessment, and the Global Reporting Initiative Standards, are indicated as useful tools to increase the standards of respect for human rights of companies required to elaborate a sustainability report following the Dir. n. 2022/2464 EU (that has succeeded to the non-financial declarations of the Dir. n. 2014/95).[30]

The Report "Understanding Voluntary Sustainability Standards" published by UNCTAD in 2023[31] remarks that the Voluntary Sustainability Standards (VSS) «are likely to become even more prominent in the coming years as several new regulatory initiatives are imposing due diligence requirements on firms».

---

[28] While the European Union is experiencing a simplification under the Omnibus Package, and the US a backtrack on sustainability policies, meanwhile, mandatory supply chain due diligence laws are being developed to make their appearance in other areas of the world. For example, in Thailand, that is drafting a mandatory supply chain due diligence law, see www.business-humanrights.org. Sustainability reporting standards requiring a double materiality assessment were published in December 2024 in China. They will be mandatory for large listed and dual-listed firms in 2026, and are receiving positive feedback, see the Guidelines No. 14 of Shanghai Stock Exchange for Self-regulation of Listed Companies. The regulation has two layers, the Chinese Corporate Sustainability Disclosure Standards (CSDS), that are the national backbone and align with global norms, and the CSR Guidelines from China's stock exchanges that are the practical rulebook. In October 2025 the South-East Asiatic countries associated in the Association of Southeast Asian Nations (ASEAN) adopted the Environmental Rights Declaration, that recognizes the fundamental rights to a safe, clean, healthy, and sustainable environment. Australia is doing steps ahead on sustainability obligations, it passed in 2025 a legislation on mandatory sustainability reporting for large entities, that New Zealand already has. At the same time, it witnessed the development of climate litigation. California is preparing to introduce the most ambitious sustainability reporting rules in the US, including non-voluntary reporting and data collection on Scopes 1, 2, 3, that obliges to an integration with the control of the supply chain.

[29] L Valle, MC Marullo, 'Contract as an Instrument achieving Sustainability and Corporate Social Responsibility Goals' (2022) 1-2 International Community Law Review 100 ff., 119 ff. See Shen, Faure (n 16) 462, who conduct an analysis based on the method of law and economics and affirm: «we found that private standardization can complement public regulation in achieving sustainability».

[30] F Gallo Perozzi, F Longo, F Bernardi and R Randazzo, *In brief: human rights compliance for businesses in Italy*, in <www.Lexology>.

[31] Available on the internet.

In fact, standards can help professionals to even know the new rules of law or can help operators in the understanding of those provisions, making it simpler and easier, can contribute to assure the access to the rules in an appropriate text for a specific economic sector, or serve to adapt the rules to a specific economic sector. [32] Furthermore, the processes structured by the certification systems, together with the goals designed by the standards, regularly prove to be of help to companies (likely even more so for SMEs, that have a simpler structure) in developing their internal organization for the purpose.[33]

The recourse to certifications as a useful tool is confirmed by a recent OECD Paper published in 2024 that affirms: «well designed and governed certifications (…) are among the many tools that companies can use to implement international human rights and environmental due diligence standards and meet emerging legislative requirements including on mandatory due diligence and sustainability disclosure».[34]

In some special sectors, such as those of timber and wood production and of agri-food production, which have long had dedicated legislation, certifications are regularly used.

The timber EU Regulation n. 995/2010, on obligation of operators «who place timber and timber products on the market» (that was preceded by EC Reg. n. 2173/2005 on import of timber in the European Union), has become effective in 2013, and has been followed by the new EU Reg. n. 2023/1115. There are very well-known certifications operating in the sector: the Forest Stewardship Council Certification (FSC) and the Program for Endorsement of Forest Certification scheme (PEFC), that are international, independent and third-party certifications. And in fact, the Guidance Document on EU Reg. n. 2023/1115 issued in August 2025 «directed primarily to stakeholders considering making use of certification or third-party verified schemes», affirms that they may consider using certification schemes. And that «given

[32] L Valle, MC Marullo, 'Contract as an Instrument achieving Sustainability and Corporate Social Responsibility Goals', cit., 120.

[33] Guidance started also to make their appearance as an useful instruments for companies, as an example see a recent "Implementation Guideline for child labour remediation case management" in Malaysia's palm oil sector (https://childrights-business.org/index.php/resources/my-voice-publishes-final-guideline-to-strengthen-child-labour-remediation-in-malaysia-s-palm-oil-sector). Another more general reference is the Practical Guide "Businesses – Affected Communities, Adopting a Human Rights-based Approach to Meaningful Engagement for Effective Impact Management", UN Global Compact Network France, launched in 2025. These Guidances do not contain standard rules but offers standardized procedures, practical tools and best practices to support case management. Private standards and private standards for certification are completely different instruments from guidances, as far as their regulatory characteristic is concerned. As experience has shown, the areas of business and human rights and environmental sustainability require voluntary standards as a necessary complement to hard form of regulation, «especially since corporate conduct cannot be easily regulated across national borders» *v se inserire anche altrove questo profilo*. Voluntary standards are part of the "smart mix" of regulatory measures supported by John Ruggie (the "father" of the UNGPs). About the "smart mix" of legal regulations and private rules, or soft law rules and private standards, Rasche (n 23) 176, concluding that «this requires that we rethink how public and private governance interact and how these interactions can be institutionalized and coordinated». About the integration of different sources of regulation in the fields of business and human rights and environmental sustainability, also L Valle, S Baroncelli 'Corporate Social Responsibility, Human Rights and Sustainable Development: Integrated Perspectives from International Law, EU law and Contract law' (2022) 1-2 Special Issue, 1-188.

[34] *OECD Alignment Assessments of Sustainability Initiatives in an Evolving Regulatory Context*, OECD Business and Finance Policy Papers (2024) 69, 6.

their potential added value [- of certifications -] in providing complementary information, such as on geolocation coordinates and supporting the operators' risk assessment undertaken as part of their due diligence exercise that relevant products are legal and deforestation-free».[35]

The applicative experience in the sector of wood and timber production shows that the recourse to a certification system is a useful tool to regulate the relationships in the supply chain, so that the buyer further down the supply chain can rely on certain production standards that the supplier should adhere to. Using a certification system can be even more useful in global commercial relations, which do not have common or harmonized legislation to share as it is the case for EU Member States.[36]

The agri-food sector is widely regulated by rules of law: a general law is EU Reg. n. 178/2002 (modified by EU Reg. n. 2019/1381), followed by EU Reg. n. 1169/2011[37] on the provisions on food information to consumers. Even in this sector, certifications are very present, as for example the BRC-Food (British Retail Consortium, necessary to export to UK), the IFS (International Food Standard), the ISO 22000 (HACCP method), the FSSC 22000 (Food Safety Certification Scheme, that merges ISO 22000 and ISO/TS 22002, and - in version 5 - merges also ISO 9001 and 14001), the organic certification in accordance with EU Reg. n. 848/2018, that entered into force in January 2022.

About conflict minerals, EU Reg. 2017/821 – entered into force on the 1st of January 2021 - introduced a due diligence obligation on Union importers of tin, tungsten, tantalum and gold, in line with the OECD Guidance for Responsible Supply Chain of Minerals from Conflict-Affected and High-Risk Areas.[38] The objective of the Regulation is to break the link between mineral exploitation and conflict financing, and to address human rights abuses in the supply chains. In this field, more set of standards complement each other to help the economic operators required to fulfill legal obligations. These are the Responsible Minerals Assurance Process (RMAP) and its facility standards of the Responsible Minerals Initiative (RMI), the Responsible Business Alliance (RBA) Code of conduct, and other key mining frameworks.[39] At the end of 2023, a joint statement by 20 NGOs has drawn the EU's attention to the difficult penetration of the legislative rules in this sector, warning against also overreliance on industry-led schemes and third-party audits. So that, while the EU Conflict Minerals Regulation represents a significant step towards responsible mineral sourcing, its effectiveness is hampered by a lack of transparency, enforcement challenges, and insufficient engagement with producing countries.[40]

[35] Guidance Document for EU Reg. n. 2023/1115, C/2025/4524, 12.8.2025, p. 22.
[36] A reported case is related to a Chinese wood supplier of Ikea, that provided certifications that were uncovered to be false, so that the origin of the wood was unknown. In fact, Ikea, that put in place a supply chain due diligence system for the entire wood supply, requires to its suppliers a certification FSC to ascertain the supply traceability.
[37] That modified UE Reg. nn. 1924 and 1925 of 2006.
[38] A Report by the EU Institutions on the EU Reg. n. 2017/821 was issued in September 2024, COM(2024) 415 final.
[39] See the website <www.responsiblemineralsinitiative.org>.
[40] See the Report Paper on the effectiveness of the EU Regulation 2017/821 IPIS, PAX, 'The EU Conflict Minerals Regulation. High Stakes, Disappointing Results' (responsiblemines) <www.responsiblemines.org>.

A possible recourse to certifications as instruments helping to comply with legislative provisions, can be found in a Guidance issued by the Danish Consumer Ombudsman about greenwashing practices. The Guidance requires that green claims that are not in contrast with legislative provisions on greenwashing shall be consistent with the lifecycle assessment process, to which the certifications under the ISO 14040, 14067, 14064 offer the methodological analysis required.

As seen, the same EU Dir. 2024/825 recognize a decisive role for certification systems, since from its entry into force sustainability labels, if not based on a legal provision, must be based on a certification system, with the characteristics we will see in the following paragraphs.

Even if this paragraph has highlighted the concrete relevance of certification systems, attested, among other things, by the fact that they are mentioned in legal regulations and various guidance and guidelines, in the final parr. 8 and 9 we will consider the current issues that need to be addressed for certification systems to fully play their role.

4. Certification schemes in the recent EU Directives and EU Directive Proposals.

The recent EU Dir. n. 2024/825 focuses on environmental claim, sustainability labels, commercial guarantees of durability and their communication to the public and deals also with certifications and their characteristics. [41] The Directive concentrates, in particular, on the communications by commercial and economic operators to the public of consumers. In fact, this Directive modifies EU Dir. n. 2005/29 "concerning unfair business-to-consumer commercial practices in the internal market"[42] and, as the Directive's title indicates,[43] it contains a regulation about unfair commercial practices, with the aim of ensuring that the labels and signs used on the market – among other practices - communicate a reliable sustainability content.

This Directive states, in its Recital 7, that sustainability labels can be used only if they are based on a certification system or on a system ruled by a public authority (as are for example EMAS and Ecolabel systems – referred to in par. 2 – that are regulated by the EU legislator).

EU Directive n. 2024/825 usefully gives a legal definition of certification, clarifying the characteristics required for the credibility of a certification, an issue that had already been questioned years ago about the Voluntary Sustainability Standards. [44] It has been reported, in fact, that «as VSS proliferated, the more rigorous initiatives became concerned about others' lack of rigorous standards, independent evaluation, benefits, impact assessment, and transparency. In 2002, they established the International

[41] For a general analysis of the EU Dir. 2024/825 (and the possible transposition in German law), see S Jung, M Dowse, 'Umweltwerbung in der EU – Quo Vadis?' 2025 (11) EuZW 506 ff.
[42] Other than the EU Dir. 2011/83 "on consumer rights".
[43] The title of the EU Dir. 2024/825 indicates the goal of "empowering consumers (…) through better protection against unfair practices and through better information".
[44] Benneth (n 19) 181.

Social and Environmental Accreditation and Labeling (ISEAL) Alliance [45] to improve VSS impact, credibility, uptake, and effectiveness by identifying best practices in social and environmental standards-setting and verification».[46]

As indicated by EU Dir. n. 2024/825, a "certification scheme" is a third-party verification scheme, that – among the other conditions - sets out procedures dealing with the non-compliance of the scheme's requirements. The procedures following the non-compliance are based on objective systems of monitoring the trader's compliance with the scheme requirements, that should be carried out by a competent and independent third party (Recital 7 and Art. 1, lett. *b*, *sub r*). For a more detailed analysis about the characteristics of certifications in EU Dir. 2024/825 see par. 5.

The Green Claims Directive Proposal focuses also on the communication of certification schemes, but not only. It deals with the issue of the proliferation of sustainability trademarks and labels and the necessity that, in the interest of the market clarity and consumers' information, the proliferation is avoided. Moreover, it introduces a "verification" procedure for the preventive assessment of claims and labels.

Both EU Dir. n. 2024/825 and Directive Proposal on Green Claims address communications based on CO2 emission reduction actions and related to climate neutrality. This is a point on which many labels and certifications make promises to the market, which are often – or, rather, most of the time – not very clear.[47]

EU Dir. n. 2024/825 focuses, in particular, on claims that create the impression that consumers can contribute to a low-carbon economy by purchasing retailers' products. Recital 4 states that «to ensure the fairness and credibility of such claims, Article 6(2) of Directive n. 2005/29 should be amended to prohibit such claims, following a case-by-case assessment, where they are not supported by clear, objective, publicly available and verifiable commitments and targets given by the trader and set out in a detailed and realistic implementation plan». In fact, as stated in Recital 8, «in cases where the displaying of a sustainability label involves a commercial communication that suggests or creates the impression that a product has a positive or zero impact on the environment, (…) that sustainability label should also be considered as constituting an environmental claim».

Recital 12 indicates that claims based on the offset of greenhouse gas emissions and asserting that a product, either a good or a service, has a neutral, reduced, or positive impact on the environment in terms of greenhouse gas emissions should be prohibited. Such claims – as "climate neutral", "CO2 neutral certified", "climate net zero", "reduced climate Impact", "limited CO2 footprint" - should only be allowed when they are based on the actual lifecycle impact of the product considered, and not based on the offsetting of

[45] ISEAL is currently a global membership organization for credible sustainability standards. It has issued Codes of Good Practice to support sustainability systems and improve their functioning.
[46] Benneth (n 19) 181.
[47] The EU is preparing the proposal for the upcoming Industrial Decarbonization Accelerator Act as a key part of the Clean Industrial Deal. The proposal is directed to accelerate the decarbonization of the Europe's energy-intensive industries, such as steel, cement, and chemicals, while ensuring that these industries remain competitive on the global stage. See 'Public Consultation for the Upcoming Industrial Decarbonization Accelerator Act' (*lexology, 1 may 2025*) <*www.Lexology.com*>.

greenhouse gas emissions outside the product's value chain, as the former and the latter are not equivalent. «Such claims should not prevent companies from advertising their investment in environmental initiatives, including carbon credit projects, as long as they provide such information in a way that is not misleading and that complies with the requirements laid down in Union law».[48] We can therefore understand that in the Directive's vision, carbon credits transactions should not be considered as actions to reduce CO2 emission, but as an investment in environmental initiatives, admitted if not misleading. The issues open by CO2 offset and its reliability relates anyway not only to claims and communication, but also to the contents and consistency of all the standards and practices operating through offsets, rather than on the actual reduction of the negative emissions. In fact, what can have a positive impact on sustainability goals is the real reduction of negative emissions and not their simple compensation, in which result the offset practices,[49] as we will see at par. 8.

A rule about certifications can be found also in the Directive on the due diligence of the supply chain, EU Dir. n. 2024/1760. Here the focus is on the objective that the adoption of a certification scheme by an entrepreneur cannot lead to dismissal for his liability, as we will see at par. 7.

Regarding certifications, EU Regulation on Eco-design (EU Reg. n. 2024/1781) at Recital 40 underlines that the EU Commission will consider, where appropriate, the development of a certification system for the digital product passport [50] service providers. Then, the development of a digital product passport service will be, possibly, under the control of a certification system.[51] Linked to Recital 40 is the provision of Art. 11.3 of the same EU Regulation.

5. EU Directive 2024/825, «Empowering Consumer for the Green Transition through better protection against unfair practices and through better information».

As seen, EU Dir. n. 2024/825 states the rule that sustainability labels can be used only if they are based on a certification system or on a system ruled by a public authority (Recital 7). «Displaying a sustainability label which is not based on a certification scheme or not established by public authorities constitutes an unfair commercial practice in all circumstances» (Recital 42). Moreover, if the

[48] In fact, the revenues from the compensation mechanism are invested in the scientific and technical development of systems to capture the CO2 from the atmosphere, and the funds invested up to now were insufficient.

[49] See C Kaupa, 'The Problem of the Carbon Credits and Offsetting in Corporate Climate Disclosure' 2025 (4) Eur. Bus. Law Rev. 573.

[50] The Digital Product Passport (DPP) is an innovation included in the EU Eco-design for Sustainable Products Regulation to store and to share relevant data on the sustainability, durability and other environmental aspects of a product. It can also host additional information, for instance product instructions or conformity documents. The DPP will help to make informed decisions and to increase the demand for sustainable products.

[51] A public consultation on the EU Commission's website – which also addressed the need for a certification system for service providers - closed in July 2025 (https://single-market-economy.ec.europa.eu/news/commission-launches-consultation-digital-product-passport-2025-04-09_en), so further developments are expected.

label does not communicate a reliable sustainable content, or communicate it in an unfair way, the use of that label could result in a greenwashing practice and be sanctioned as an unfair commercial practice under the regulation of EU Dir. 2005/29 as amended by EU Dir. 2024/825.

It is very important that the Directive provides a legal definition of "certification scheme", as certification systems can be organized in many different ways and have different characteristics, starting for example from audit processes, as seen above in par. 2.

Concerning the characteristics of a certification, lett. *r*) of the new Art. 2 of Dir. n. 2005/29 (modified by art. 1, Dir. n. 2024/825) states that a "certification scheme" is «a third-party verification scheme that certifies that a product, process or business complies with certain requirements, that allows for the use of a corresponding sustainability label, and the terms of which, including its requirements, are publicly available and meet the following criteria:

(i) the scheme is open under transparent, fair, and non-discriminatory terms to all traders willing and able to comply with the scheme's requirements;

(ii) the scheme's requirements are developed by the scheme owner in consultation with relevant experts and stakeholders;

(iii) the scheme sets out procedures for dealing with non-compliance with the scheme's requirements, and provides for the withdrawal or suspension of the use of the sustainability label by the trader in case of non-compliance with the scheme requirements;

(iv) the monitoring of a trader's compliance with the scheme's requirements is subject to an objective procedure and is carried out by a third party whose competence and independence from both the scheme owner and the trader are based on international, Union or national standards and procedures».

The definition of certification scheme is given by the Directive in the context of the unfair commercial practices regulation, in which certifications have the role of supporting the credibility and transparency of sustainability labels, as explained in Recital 7 of Dir. n. 2024/825. The Recital says that it is appropriate to prohibit the use of and the communication through sustainability labels that are not based on a certification scheme - understood in line with the definition seen here above - or that have not been established by public authorities. The system ISO 24010 is cited as a possible example of a standard basis for an accepted certification system (Recital 10).

Before displaying a sustainability label the «trader» (i.e. the business) should ensure[52] that the publicly available terms of the certification scheme meet the minimum conditions of transparency and credibility (in line with the provisions in the text of Art. 2, lett. i and ii, seen above).

Moreover, the «trader» should ensure that a system of objective monitoring of compliance with the requirement of the scheme, carried out by a third independent party, is in place (in line with the provisions in the text of Art. 2, lett. iv, seen above).

The monitoring system should operate in compliance with international, Unional or national standards and procedures, such as the international standard ISO 17065 on conformity assessment (containing requirements for

[52] This follows the general provision of EU Dir. 2005/29 that at Art. 5.2 (a) states that an unfair commercial practice is a practice «contrary to the requirements of professional diligence».

the organizations certifying businesses, processes, and services), or through the mechanism provided for by EU Reg. n. 765/2008, which establishes the rules for the accreditation of product conformity assessment bodies (Recital 7).

As said, the use of, and the communication through, sustainability labels is possible, when a certification scheme is missing, when such labels are established by a public authority, or when they are used in accordance with the art. 35 of Reg. n. 1169/2011 EU on food information to consumers. Examples of sustainability labels established by public authorities are – as said – the logos awarded in compliance with the requirements of EC Reg. n. 1221/2009, about EMAS, or EC Reg. n. 66/2010, about Ecolabel.

In conclusion, from the legal provisions regarding certifications contained in EU Dir. n. 2024/825, the following key points can be identified:

- certification schemes need to be clear and transparent in the way they communicate their sustainability contents to the market and consumers;
- the terms of the certification schemes should be developed by the scheme owner in consultation with relevant experts and stakeholders and be publicly available;
- they should be third-party verification schemes, by a competent and independent body;
- procedures for dealing with non-compliance with the scheme requirements have to be in place;
- certification schemes cannot result in a dismissal of the responsibility and liability of the interested company, either in the sense that companies cannot use certifications as a way to hide unsustainable contents under the appearance of a sustainable practice (for example, when the certification rely on systems based on "CO2 neutral" certified practices, when this claim is not supported by clear scientific proven evidence of its positive impact), either in the sense that they cannot rely on the role of certifications to dismiss their liability (the explicit reference on this last point is in EU Dir. 2024/1760);
- it is necessary to avoid the proliferation of certification schemes - which is an issue expressly addressed by the Green Claim Proposal Directive[53] - as an application of the transparency principle, and a way to prevent greenwashing.

6. The EU Proposal for a Directive on Green Claims.

EU Directive Proposal on Green Claims – that affirms to be a *lex specialis* to EU Dir. n. 2024/825 – deals with environmental claims and with certifications (to which the Directive Proposal refers mostly with the words "environmental labelling schemes" [54]) as systems that communicate to the public through the environmental labels.[55]

[53] About that point see the next par.

[54] The Directive Proposal uses the expression «environmental labelling schemes», affirming that it means «a certification scheme which certifies that a product, a process or a trader complies with the requirements for an environmental label» (art. 8).

[55] On the Proposal, see S Jung, M Dowse, 'Key Aspects of the Green Claims Directive Proposal' 2024 1 EuCML 11 ff. The finalization of the Proposal is expected to take place at the latest in 2026.

The legislator specifically focuses on the proliferation of environmental labels which aim to prove sustainability contents, and on the possible lack of transparency of the environmental labelling schemes. For that reason, EU Dir. n. 2024/825 – as seen in the previous par. - and the Directive Proposal on Green Claims indicate the need that labels are based on a certification scheme as defined in the new Art. 2 lett. r) of EU Dir. n. 2005/29, or, alternatively, established by public authorities.

Recital 39 of the Directive Proposal reports that in the EU market are currently in use more than 200 environmental labels, that differ greatly in their functioning. They differ for example in the transparency and comprehensibility of the standards, or the methods used, the frequency of revisions, and the level of auditing and/or verification. These differences affect the reliability of the information communicated by the environmental label.

Since evidence suggests that many environmental labels currently used on the EU market are misleading and, in particular, many environmental labels «lack sufficient verification procedures», Recital 39 continues stating that «explicit environmental claims made through environmental labels should be based on a certification scheme».

Recital 42 recalls the text of EU Dir. n. 2024/825 according to which – as seen above, at par. 5 - «displaying a sustainability label which is not based on a certification scheme or not established by public authorities constitutes an unfair commercial practice in all circumstances». «This means that the "self-certified" sustainability labels, where no third-party verification and regular monitoring takes place as regards compliance with the underlying requirements of the sustainability label are prohibited».

In Recital 42 the Directive Proposal recalls that the very concept of certification requires (in line with the definition of the new Art. 2 lett. *r*) of EU Dir. n. 2005/29, as seen above at par. 5):

- the verification of compliance by a third-party; and
- the regular monitoring by a competent and independent third party.

Recital 44 affirms that «in order to avoid further proliferation of national or regional officially recognized EN ISO 14024 type I environmental labelling ("ecolabelling"), and other environmental labelling schemes, and to ensure more harmonization in the internal market, new national or regional environmental labelling schemes should be developed only under the Union law. Nevertheless, Member States can request the [EU] Commission to consider developing public labelling schemes at the Union level for product groups or sectors where such labels do not exist yet in Union law and where harmonization would bring added value to achieve the sustainability and internal market objectives in an efficient manner».

In fact, «environmental labelling schemes established by private operators, if too many and overlapping in term of scope, may create confusion in consumers or undermine their trust in environmental labels. Therefore, Member States should only allow that new environmental labelling schemes are established by private operators provided that they offer significant added value as compared to the existing national or regional schemes in terms of environmental ambitions of the criteria to award the label, coverage of the relevant environmental impacts, and completeness of the underlying

assessment» (Recital 46). Consequently, the creation of new labels - and certifications - should be seen as something to be developed based on necessity or usefulness, taking into account harmonization at European level, and should otherwise be avoided.

The EU Commission will publish, and keep up-to-date, a list of officially recognized environmental labels that are allowed to be used on the Union market after the date of the entering into force of the Directive (Art. 8, par. 7).

Regarding the characteristics of environmental labelling schemes, Art. 8.1 states that «environmental labelling scheme means a certification scheme which certifies that a product, a process or a trader complies with the requirements for an environmental label». And that «only environmental labels awarded under environmental labelling schemes established under Union law may present a rating or score of a product or trader based on an aggregated indicator of environmental impacts of a product or trader».

Art. 8.2 of the Directive Proposals states that environmental labelling schemes – that is to say certification schemes - shall comply with the following requirements:

(a) the information on the ownership and the decision-making bodies of the environmental labelling scheme is transparent, accessible free of charge, easy to understand and sufficiently detailed;

(b) the information about the objectives of the environmental labelling scheme and the requirements and the procedures to monitor compliance of the environmental labelling scheme are transparent, accessible free of charge, easy to understand and sufficiently detailed;

(c) the conditions to join the environmental labelling schemes are proportionate to the size and turnover of the companies, in order not to exclude SME;

(d) the requirements for the environmental labelling scheme have been developed by experts that can ensure their scientific robustness and have been submitted for consultation to a heterogeneous group of stakeholders that has reviewed them and ensured their relevance from a social perspective;

(e) the environmental labelling scheme has a compliant and dispute resolution mechanism;

(f) the environmental labelling scheme sets out procedures for dealing with non-compliance and the withdrawal or suspension of the environmental label in case of persistent and flagrant non-compliance with the requirements of the scheme.

The indicated characteristics of an environmental certification scheme are therefore in line with the requirements of EU Dir. 2024/825, and complement them.

If the proposed Green Claims Directive is approved, and approved in its current text, environmental labels, as well as environmental claims, will be subject to a system of preventive verification. That will be implemented in accordance with the procedure set out in the Directive Proposal, which guarantee compliance with Artt. 3 – 7 of the Directive Proposal (Art. 10)[56]. The

[56] The verification system has a central role in the Directive Proposal, and has also been criticized for being too difficult to comply with and costly, despite the recognition of simplified obligations for SMEs and exemption for the system for microenterprises.

verifier shall be a third-party conformity assessment body, accredited in accordance with EU Reg. n. 765/2008 (Art. 11).

7. Certification schemes and the Corporate Sustainability Due Diligence Directive (CSDDD).

Further certification regulations can be found in EU Dir. n. 2024/1760 on Due Diligence of the Supply Chain, for the case in which the company uses a certification system to support its due diligence obligation. In fact, supply chain control activities can be subject to a certified process such as, for example, a process based on the ISO 28000 for the Supply Chain Security Management.

Art. 29, par. 4 of EU Dir. n. 2024/1760 states that «companies that have participated in industry or multi-stakeholder initiatives, or used independent third-party verification or contractual clauses to support the implementation of due diligence obligations may nevertheless be held liable in accordance with this Article».

The aim of the Directive is therefore to ensure that companies are always responsible and obliged to respect rights and resources along their supply chain, while the adhesion to collective agreements or the recourse to certification systems cannot be used to evade their responsibility and obligation as regulated by the Directive.

8. The current state of standards and certification schemes under the EU Green Deal legal framework and the Clean Energy Development Plan.

Following the entry into force of the new national regulations in European countries and the EU rules mentioned at the end of par. 2, doing business in compliance with sustainability goals has begun to become mandatory for economic operators[57] and, given the symptoms of climate change we are experiencing in the reality, also urgent, in the general interest.

The series of legislative acts addressing sustainability objectives has become significant, even if some important legal regulations are currently interested by a process of "simplification" and revision, under the so-called "Omnibus Package". Those are the CSRD (EU Dir. n. 2022/2464, already transposed in the Italian legal system by d.lgs. n. 125/2024), the CSDDD (EU Dir. n. 2024/1760), the Taxonomy Regulation (EU Reg. n. 2020/852) and the Carbon Border Adjustment Mechanism (CBAM, which entered into force on the 1st October 2023, but whose definitive period begins on the 1st of January 2026). At the same time a new plan, the Clean Energy Development Plan (issued in autumn 2024) focusing on circular production and clean energy, indicates a

[57] This affirmation is certainly general, but it corresponds to reality if we take into account the number of legal regulations in various economic sectors and the current developments in climate litigation, which we will see in this par. However, the obligations are different for large companies– which are more affected by legal obligations - and for small-medium enterprises, and differ across economic sectors.

sustainability path less concentrated on supply chain due diligence and more on the development of a circular production system and a circular economy.[58]

In any case, we must consider that there already exists a large set of legislative acts that indicate or impose sustainability objectives: those are, for example and not exhaustively, EU Dir. n. 2024/825[59] empowering consumers toward the green transition, EU Directive on the consumers Right to Repair (EU Dir. n. 2024/1799) [60], the deforestation legislation with EU Regulation n. 2023/1115 (EUDR)[61], the Regulation that bans the forced labor products (EU Reg. n. 2024/3015, amending the EU Dir. n. 2019/1937), EU Regulation on Eco-design that - among others - establishes rules on the Digital Passport (EU Reg. n. 2024/1781), EU Regulation on nature restoration (EU Reg. n. 2024/1991, amending EU Reg. n. 2022/869) about the restoration of the biodiversity, the Battery Regulation (EU Reg. n. 2023/1542), the Sustainable Finance Disclosure Regulation (EU Reg. n. 2019/2088), the Conflict Minerals Regulation (EU Reg. n. 2017/821).

All those legal regulations indicate a direction towards sustainability and protection against climate change that cannot be ignored, that we can find expressed also by very general principles and rules of law. Such as those of the EU Charter of Fundamental Rights (Art. 37 on environment protection, Art. 31 on fair and equal working conditions, Art. 32 on prohibition of child labor), those contained in the Paris Agreement of 2015, and now also expressed by principles included in national Constitutions (see for example, in Italy, Artt. 9 and 41 of the Constitution, in Holland, Art. 21 of the Dutch Constitution). So that, the last progress towards a revision of the CSRD and CSDDD with the postponement of some obligations by EU Dir. n. 2025/794 (Stop-the-clock)[62], and the simplification of some obligations (still in progress to be approved through a normal – and not urgent - legislative process) does not unequivocally mean that sustainability goals will play a less important role in the near future than before.

Indeed, it is necessary to consider both the significant number of existing regulations and the fact that they are in force in legal systems in which some general principles have incorporated the orientation towards the achievement of sustainability goals. Moreover, as we have seen above, national legislations are already in force in different European countries, as those on companies' due diligence obligation on their supply chain, as it is in France, Germany, UK,

[58] When discussing circular manufacturing and circular economy, it is important to note that not every type of circular manufacturing approach is associated with lower carbon emissions and potential climate mitigation outcomes, but only the "product redesign" strategy is associated with lower levels of scope 1 and scope 2 emissions, M Molinaro, G Orzes, J Sarkis, 'Unpacking Circular Economy Practices and Carbon Emission Relationships: co-benefits and Legitimacy Perspectives' 2025 Business Strategy and the Environment, 1-22.

[59] Not transposed yet.

[60] Not transposed yet.

[61] This Regulation guarantees that the products consumed by EU citizens do not contribute to deforestation or to forest degradation worldwide. The EU Reg. n. 2023/1115 repealed the previous important EU Reg. n. 2010/995 known as EU Timber Regulation (EUTR). The entry into force of the Regulation provisions have recently been postponed, for large and medium operators to the 31st December 2026, and for micro and small operators to the 30th June 2027.

[62] About which see, for example, G Bova Crispino, 'La CSDDD e la centralità del contratto come strumento di conformazione di un mercato unico europeo sostenibile' in G. Cassano, G. Capo, F. Costantino (eds.) *I Principi ESG e di sostenibilità* (Lefebvre Giuffré 2025) 69 f.

Netherland, Norway.[63] Therefore, foreign companies that are in commercial relationships with operators from those countries may be required – and regularly they are – to follow the standards arising from their legislations.

At the same time, progress towards circular production and eco-design of products is confirmed, for example by EU Regulation on Eco-design, EU Directive on the Right to Repair and some recent EU regulation proposals. Such as the Proposal about the Circular Economy Act (CEA) – due for adoption in 2026 – that aims at substantially improving the EU's economic security, resilience, competitiveness and decarbonization, establishes a single market for raw materials, increases the supply of high-quality recycled materials and stimulates the demand for these materials in the EU. The importance of assessing sustainability and climate change-related risks is currently evident in the financial sector. Banks continue to make further efforts to require the integration of ESG standards into business and management processes in line with the "EBA Guidelines on the Management of ESG Risk", that will become effective from 2026 for the bigger banks, and from 2027 for the smaller ones. In fact, ESG risks are reputed to influence the financial risk, and for that reason business enterprises are called to give more complete ESG information, among which data on greenhouse gas emissions, sustainable transition strategies and compliance to social and governance standards.[64]

A further element that confirms the importance of environmental and fundamental rights protection from climate change in legal systems[65] is the definitive affirmation of judicial cases of "climate change litigation"[66] in several countries, at European and international level.[67] In April 2024 the European

[63] Last information says that Germany and France would like to revise their internal law, the law on the *Devoir de vigilance* (2017) and the *Lieferkettegesetz* (2021). At the beginning of September 2025 the German Ministry of Labour and Social Affairs has published a draft amendment to the *Lieferkettengesetz* (LkSG) (see, www.bmas.de). Differently, a report about the application of the law in Norway (that entered into force in 2022) called "Non-paper" and addressed by the Norwegian Government to the EU Commission for the revision of the CSDDD, namely a Non-paper on the omnibus proposal, refers to an improvement of firms' supply chains and better supply chain management through the identification of significant risks after the application of the law. The report expresses the intention to continue to align with the UNGPs and the OECD Guidelines. On the other hand, the Paper also highlights that implementation can be challenging and that some companies perceive an increased administrative bu rden, https://www.regjeringen.no/contentassets/8b339b37f1ea48aa891dc0302ff0439b/norwegian-non-paper-on-the-omnibus-i-proposal-com-2025-81l1393877.pdf

[64] On the "EBA Guidelines on the management of environmental, social and governance (ESG) risks", see the "Final Report", EBA, EBA/GL/2025/01, 8.1.2025.

[65] The protection of the environment has been expressly acknowledged as a fundamental right of persons by the General Assembly of the United Nations in 2022, and already in 2021 the German Constitutional Court affirmed environment protection as a fundamental right of persons with reference to Art. 20a of the *Grundgesetz*, stating the right to a sustainable climate future and an intergenerational responsibility.

[66] On the interaction and possible convergence between due diligence legislation and climate change litigation to strengthen corporate climate change accountability, M Rajavuori, A Savaresi, H van Asselt, 'Mandatory due diligence laws and climate change litigation: Bridging the corporate climate accountability gap?' (2023) Regulation & Governance 944 ff. In the current uncertain time, we might consider climate change litigation a potential temporary substitute for due diligence legislation to help achieve sustainability goals.

[67] B Pozzo, 'Il contenzioso climatico nel prisma del diritto comparato' (2024) 4 Dir.Pubbl.Comp.Eur. 987 ff., addressing the origins of climate change litigation in the US and Europe, and observing that the climate change in Europe has found its reason for developing in the ineffectiveness of our legislative framework, together with the growing concern of environmental organizations.
The world's first decision ordering States to limit greenhouse gas emissions for reasons other than statutory obligations was issued in the case *Urgenda Foundation v. the State of the Netherlands*. The decision by the Dutch Supreme Court in December 2019 is based on art. 162 of the Dutch Civil Code (the rule corresponding

Court of Human Rights affirmed, in the case Klimaseniorinnen v. Switzerland, that this country had not made sufficient efforts to pursue the climate goals set out in the Paris Agreement. The European Court recognized a right to be protected against the climate change and its negative effects, on the ground of the right to a safe environment based on the right to life (art. 2, European Convention of Human Rights) and on the right to respect for private and family life (art. 8, European Convention of Human Right).[68] Climate litigation is registering also cases against companies, about the reduction of emissions, the requests for damages and the affirmation of the violation of human rights, such as the rights to life, health, undisturbed private life. Public authorities and business enterprises can then be held accountable for their inaction - or insufficient action - in achieving the objectives set at international level, by the Paris Agreement, or at EU level.[69] An Opinion by the International Court of Justice in the case filed by Vanuatu, given on the 23rd of July 2025 (that is a non-mandatory opinion, but a very important reference point for climate change lawsuits), affirmed that States that fail to comply with their climate change obligations commit a tort and may be held liable for damages caused to States most affected by climate change.[70] Moreover, the International Court of Justice affirmed in July 2025 that human rights, including the right to a clean, healthy, and sustainable environment, form the foundation of States' obligations to address climate change. It affirmed also the very important

to our art. 2043 c.c.), and art. 21 of the Constitution of the same country, read in the light of artt. 2 and 8 of the European Convention on Human Rights. Pozzo (n 67) 989; L Serafinelli, *Responsabilità extracontrattuale e cambiamento climatico* (Giappichelli 2024) 57 ff. In this decision we can see that artt. 2 and 8 of the European Convention produce their effect through a general rule of the civil code, integrating its content. For the direct or indirect effect of general principles or general rules of law - as those in the European Charter of Fundamental Rights or in national constitutions - in the horizontal relationships of private law, here about fundamental rights protection and damages arising from tort, see L Valle, *Il contratto e la realizzazione dei diritti della persona*, cit., 58, about private relationships of contract law. For the effect of international legal rules and conventions – including the European Convention of Human Rights – see Valle (n 67) 349, and note 82 and 83, see also note 46 at 94 ff. with regards to the European Convention of Human Rights.

[68] Cfr. Pozzo (n 67) 61 ff.

[69] See for example a recent Italian case by the Italian Supreme Court, Cass., ord. 21.7.2025, that affirmed that the Italian judges have jurisdiction on climate litigation cases, including those involving emissions from the company's (in this case it was Eni) foreign subsidiaries. The lawsuit was brought to court by some NGO and citizens demanding a reduction in emissions, along with a request for damages and a recognition of the violation of fundamental human rights to life, health and undisturbed personal life. About the duty of care of companies, see the recent developments in case decisions, in D Lawne, A Cooper, K Elias, 'Summer review: a watershed moment for climate litigation' (Lexology 26 august 2025) <www.Lexology.com>. Cases cited are: *Lliuya v RWE*, decided in May 2025 by the Regional Court of Hamm in Germany; *Milieudefensie s Shell*, decided in November 2024 by the Hague Court of Appeal and followed by an appeal and new claims; *Ogale & Bille Communities v Shell*, decided in June 2025 by the UK High Court, followed by a report on "aligned" and "non-aligned" litigation. About the duty of care by public authorities, the article mentions the cases *Held v Montana*, decided in December 2024 by the Montana Supreme Court, and *Torres Strait Island v Australian Government*, dismissed by the Federal Court.
About the position of business enterprises, see the articles in the collective books E. de Jong (ed.) *Corporate Accountability and Liability for Climate Change* (Elgar Publ. 2024). On the organization of sustainability management, in particular in German companies, see S Jung, C Siebeck, 'Green Governance als Hebel für eine nachhaltige Entwicklung deutscher Aktiengesellschaften' (2025) NZG 1555-1561.

[70] It will however be necessary to ascertain a direct causal link between the unlawful act and the damage, which is difficult, but not impossible, as the Court stated. The UN had asked to the Court to answer to two questions: which obligations have the States along international law, to protect the earth from the greenhouse gas emissions, for the purpose to protect the present and future generations? What are the legal consequences of such obligations for States that cause environmental damage, particularly for low-lying insular States?

principle that climate treaties inform the content of customary international law, and vice versa. In this way, States that are not party to climate agreements could still be bound by the customary international law obligations defined by the treaty regime, and have the burden of demonstrating compliance. This Opinion adds to the Advisory Opinion issued on the 3rd of July 2025 by the Inter-American Court of Human Rights (IACtHR) about the nature of the right to a healthy climate, the legal personality of nature, and the obligation not to cause irreversible damage to the climate and the global environment, as a norm of *jus cogens*. The Advisory Opinion confirmed a climate-focused reparations regime, the development of a *pro-natura* principle of interpretation of international obligations, the *nexus* between investment law, climate, human rights, and associated procedural rights.

As seen above in par. 3, standards and certifications based on those standards can be of help in applying practices and organizational methods in line with the sustainability objectives established by legal rules and principles. If required by law, compliance with a standard and the related certification may even be necessary, as indicated for example in art. 11.3 of the Eco-design Regulation and by EU Dir. 2024/825 itself, which states that sustainability labels not based on a certification scheme – or not established by public authorities – should be prohibited as an unfair commercial practice, «by including such practices in the list in Annex I to EU Dir. n. 2005/29» (Recital 7).

However, at the present time, for this role of standards and certifications to become fully operational and effective, significant preventive challenges must be overcome.

First, regarding their sustainability contents, since, starting from the standards on which they are based, certification systems are not always in line with the requirements of the new EU legislation and its sustainability goals, as we will see below. Second, as regards their structure and operation, since they are not always in line with the requirements established for certification systems by EU Dir. n. 2024/825 and Green Claims Directive Proposal, as already seen in the previous paragraphs.

In terms of their content, certification systems – and even the standards on which they are based – may not be aligned with real sustainability objectives.

For example, it is well known that some certification systems are based on practices that only *prima facie* appear virtuous in term of CO2 emissions, and compliant with rules with sustainability objectives. In reality, they are simply based on carbon credits offset and therefore do not directly contribute to combating climate change, for several reasons.[71]

As regards CO2 emissions, art. 3 of Green Claims Directive Proposal, at lett. *h*), states that in the assessment of environmental claims it is necessary to «specify whether those offsets relate to emission reductions or removals, and describe how the offsets relied upon are of high integrity and accounted for correctly to reflect the claimed impact on climate».

Recital 21 of Green Claims Directive Proposal highlights the difficulty of measuring carbon offsets, as the methodologies adopted are diverse and not always accurate, transparent and solid. Most important, it affirms that to

[71] Important and serious issues related to these certifications are reported by T Fischer, H Knuth in the German magazine *Die Zeit* with an article translated and published in Internazionale, 27 January 2023, 38 ff.

contribute efficiently to the mitigation of climate change, instead of relying on offsets, businesses should prioritize the effective reduction of the emissions across their own operations and value chains. Consequently, the compliance to those standards that rely on offsets, and the certifications based on those systems that follow carbon offset practices, does not assure the objective of substantially contrasting the climate change and reducing polluting emissions.

It has also been recently stated in the literature that «research shows that carbon credits are typically not effective[,] (…) since they do not deliver the climate benefits they claim to achieve, and are therefore not equivalent to real emission reduction or removal».[72]

Another example of issues arising from the contents of the standards themselves can be found about the ISO 26000 standard [73] and its relationship with the UN Guiding Principles on Business and Human Rights (UNGPs),[74] which are a very important point of reference in the sector, to which important legal instruments are also aligned, such as the EU Dir. 2024/1760 (CSDDD).[75] In the case of ISO 26000 standard, this alignment depends on how the standard terms are implemented by companies, as the ISO 26000 system itself is considered "too broad" and "too generic" to have a transformative and disruptive effect on traditional business practices.[76] In conclusion, it can be assumed that the reference by a company to a standard such as ISO 26000 does not guarantee substantial alignment with sustainability goals.

The above suggests that existing sustainability standards should be reviewed in light of the recent legal framework having sustainability objectives.

The revision of some standards is already in progress, as the revision of ISO 14067 on product carbon footprint and ISO 14064-1 on organization carbon footprint. At the same time, new standards for sustainability goals and/or to contrast climate change, such as the carbon neutrality standard ISO 14068-1:2023, have recently been developed, or are in the process of being released, such as the net-zero standard ISO 14060.

Furthermore, it can be observed that if the content of standards and certification clauses is in contrast with legal provisions, the consequence is that such clauses are null. It is important to note that this can operate as a conflict

---

[72] Kaupa (n 49) 573 examines how the various instruments regulating corporate climate disclosure deal with carbon credits and offsetting.

[73] See also *supra*, note 14.

[74] The UNGPs (United Nations Guiding Principles on Business and Human Rights) were adopted by the Council of Human Rights of the United Nations in 2011 and are reputed as the leading global standard about business and human rights. They consist of soft law rules, but also by some rules that recall international law, already mandatory as such. They qualify themselves as rules to follow, and not just as a persuasive tool.

[75] The EU Directive on the due diligence of the supply chain (CSDDD) itself is drafted on the basis of the UNGPs and its principles, about which see *above*, the previous note.

[76] S Bijlmakers, *No ISO fix for human rights: a critical perspective on ISO 26000 guidance on social responsibility* (2021) 228, affirms that also the fact that the standard has not been updated since 2010 [even if the Italian version is of 2020], determines that it is out of date, considering the rapid changes in the CSR (Corporate Social Responsibility) field.

Despite the negative aspects recently highlighted, Bijlmakers reports that ISO 26000 has been considered a powerful statement on the moral and practical issues facing companies and other organizations, which makes valuable contributions to the realization of human rights, especially in developing countries (p. 205, citing A Henriques, 'ISO 26000: A Standard for human rights?' (2010) Sustainability Accounting, Management and Policy Journal, 103-105). Bijlmakers however concludes that «ISO 26000 has not been an impactful tool for human rights», and that «its substantive guidance seems to be out of tune with the UNGPs».

with specific legal provisions, or may even operate as a conflict with the general principles of climate change protection established by very general provisions of law, such as artt. 9 and 41 of the Italian Constitution. These last cases may be more difficult to identify and evaluate due to the very nature of the general principles, which require a greater role from interpreters.[77]

Following a private law approach, the possible nullity of standards and certifications' terms due to conflict with the contract consideration can be also considered. Being certification systems based on contracts, that can occur if the contract terms contradict the sustainability goal, as the purpose stated by the certification.[78]

9. Conclusion.

The analysis in the previous paragraphs shows that a new course for sustainability standards and certification systems is needed. To this new course contribute, as a starting point, EU Dir. n. 2024/825,[79] and will contribute, if approved, the EU Green Claims Directive Proposal. This conclusion will be further argued in the course of the paragraph.

The most important indications for the future of sustainability standards and certifications, as stated by EU Dir. 2024/825 and by Directive Proposal on Green Claims, seems to be those relating to:

- the transparency of the systems (on which the EU Dir. 2024/825 and the Green Claims Directive Proposal),
- the third-party control by a competent and independent body, and the continue monitoring of the operators' compliance (on which the EU Dir. 2024/825 and the Green Claims Directive Proposal),
- the determination of measurable contents in standards and certification systems (not explicitly directly addressed by the EU Dir. 2024/825 and the Green Claims Directive Proposal)
- the revision of the content of standards and certifications in line with the legal provisions on sustainability goals and with the most important set of rules at the international level, the UNGPs and the OECD Guidelines, which are a benchmark also for legislators. [80]

In addition to the points outlined above, which concern legally relevant issues, it must be added that the effective use of certifications requires a significant change in the mindset of many operators. Indeed, operators'

[77] For the direct effect of constitutional legal norms see Valle (n 67) 48 ff., where bibliographic references.
[78] This can be considered a general principle of contract law, identified in a famous case, the French case *Chronopost*, on which L Valle, *L'inefficacia delle clausole vessatorie* (Cedam 2004) 377.
[79] The B-Corp certification was revised after the entry into force of EU Dir. 2024/825, with the introduction of the assessment by a third-party.
[80] On the UNGPs, see *above*, note 74. The OECD Guidelines for Multinational Enterprises 1st version was released in 1976, in the 2011 edition a chapter on the protection of human rights was added (chapt. IV, which has as its reference the UNGPs), the most updated ed. is of 2023. UNGPs and OECD Guidelines are considered the most important benchmarks for the protection of human rights and environmental resources in the business activities at the international level, and have imposed themselves for the high reputation of their issuers and their moral suasion. They are regarded as sets of "soft law" rules, but a certain number of their rules come from already binding international treaties or custom international rules protecting human rights and natural resources.

attitude and purpose towards certifications cannot be of mere compliance and simple ticking-the-box, but must instead focus on satisfying the substance of the requirements for sustainability objectives.[81] That shift in mindset is something that still needs to be built on a broader level. Even if it seems likely that doing business through processes and objectives that are not aligned with sustainability goals will soon become unacceptable from a risk management perspective.[82]

As regards the indication on transparency, as can be understood from EU Dir. 2024/825, this seems to play the role of principle in the sector, as it is reiterated several times, in more diverse applications and meanings. The transparency of the labelling schemes on the information about the objectives of the environmental labelling scheme, and the requirements and procedures to monitor compliance of the environmental labelling scheme, are stated also by art. 8.2 *b*) of the Directive Proposals on Green Claims.[83]

As a first application of the transparency principle, transparency means that the terms of the certification schemes should be publicly available (art. 2, lett. *r*, Dir. 2005/29 as modified by art. 1, Dir. 2024/825), so that it is possible to have knowledge of the certification's standards. First of all, at the advantage of the contract counterparts; as they are standard terms, they might not be included in the text of the contract but they need to be knowable. And also of the consumers as final contractors,[84] and in the general interest of the market to which they communicate certain contents becoming recognizable through the labels.[85]

The possibility for consumers and for the market in general to know the certification's terms and the standards on which the certification is based is essential for the complete and clear communication of the sustainability

[81] See, for example, Podrecca, Sartor (n 64) 30, about ISO 9001.
It has been observed that a tick-box for sustainability reports is a kind of oversight that might have gone unnoticed a few years ago, but not today. The problem that we are currently witnessing is that the diluting of the CSDDD Directive and the US backlash opened a vacuum, in which too many companies are mistaking uncertainty for a reason to delay, "*Human rights due diligence inaction*" authored by T. Kramlova, T. Trier Hansen, P. Moloney, Ramboll Management Consulting, 2025, *online*.

[82] For those companies that operate at risk of violating human rights, see T Kramlova, T Trier Hansen, P Moloney, *Human rights due diligence inaction*, 2025, online: «responsible business conduct is rapidly becoming a baseline requirement for market access, financing and license to operate». It is not only the field of business and human rights that should be concerned about human rights violation, since some involvement with human rights is always present in the activity of a business enterprise, especially when we consider workers' rights. P Taticchi, *Sostenibilità e innovazione* (Dedalo 2025) 13, states that sustainability concerns financial risk: sustainability issues transform into reputation issues, and reputation issues into financial issues. Risk management is also regulated for public administration activities. In the Italian legal system, see d.lgs. n. 103/2024, that states that the control system is based on voluntary risk identification. The definition of low risk takes into account different parameters, including having a certification on ESG factors, among others.

[83] On transparency of information about the ownership and the decision-making bodies of the environmental labelling schemes, see lett. *a*) of the same article.

[84] We can think to the fact that the terms of the standards integrate the contract's content and can also determine, for example, some characteristics of the object of the contract. See for example the case of a wood production certification, as a certification FSC (Forest Stewardship Council), which guarantees that the wood comes from ecologically managed forests and from a specific area with traceability along the entire supply chain.

[85] Regarding the application of the standard ISO 14001, L Maurin, *Contrat et Droits Fondamentaux*, cit., 369, reports that the major critique to the rule ISO 14001 is the lack of transparency, in the sense that the audit results are not necessarily made public. This issue seems to be satisfied by the European reference EMAS. On ISO 14001 and EMAS see Podrecca, Sartor (n 64) 33 ff.

practices adopted. In fact, only by reading the terms of the certifications together with the standards on which they are based it is possible to understand the characteristics of the certification systems as a whole.

A particularly important concern is the transparency of the standards on which certification systems are based - that is to say, the possibility of openly accessing them - since this application of the transparency principle is not explicitly addressed.

The fact that the new legal provisions about certification systems - on which sustainability labels are based – repeatedly enphasize the issue of transparency of terms and procedures, seems to allow the interpretation that the standards on which certifications are based must also be transparent and accessible to the public. In that sense, could be understood the provision of Green Claims Proposal which affirms that the «objectives of the environmental labelling scheme» must be possible to be known. In fact, without the knowledge of the standards, the whole objective of the scheme would remain (at least partly) hidden. The public availability of standards is currently not a reality, as standards – such as the most well-known ISO standards for example - are commonly available on the market only for purchase. This appears to be a situation that deserves a decisive change from the past, considering the use and future role of standards and certifications.[86]

If we interpret the legislative requirement for transparency as including, in addition to the transparency of the certifications standards, also the transparency of the standards on which the certification systems are based, then we read the words "certifications standards" as referring not only to the terms of the certification contracts (i.e. the standard terms of the certifications) but also to the underlying standards themselves. In fact, in practice it happens that when we talk about a certification, for example "ISO 14001 certification", we refer to the standard together with the certification system, and not just the certification itself or not only the standard alone.

Connected to the transparency issue is also the problem of the exaggerate number of certification systems available, expressly addressed by Green Claims Proposal Directive. An excessive number of certification systems available can lead to greenwashing, while on the contrary a limited number of schemes could open up competition issues, due to the consequent possibility of influencing competition on the market as a consequence of the few certification schemes available.[87]

Transparency also means ensuring that the terms of the certification systems and of standards are understandable, based on their scientific consistency and coherent development.

These conclusions arise from the provisions of EU Dir. n. 2024/825 and Directive Proposal on Green Claims, that are rules contrasting unfair commercial practices. They come also from very general rules of contract law, such as the general rules on standard contract terms regulation (EU Dir. n.

[86] A debate is open among professionals about the free accessibility to the public of the ISO carbon accounting standards, see at the London Climate Action Week of June 2025, the event with D Pernigotti and R Poivet "Free Access to ISO GHG Accounting Standards". One concern highlighted is that if the standards are not freely available they will be not taken into account across the world, and their use will inevitably decline.

[87] See Shen, Faure (n 16) 462.

93/13) that stress the transparency of the contract terms elaborated by one contract part only. In fact, standards on which certifications are based, and standards that regulate the certification itself, are standard contract terms.

Labels that communicate the use of the certification scheme have also to be used in a transparent way, following the general regulation on unfair commercial practices of EU Dir. 2005/29. This Directive has been amended for the protection against unfair practices in the green transition (such as greenwashing practices) by EU Dir. n. 2024/825 and Green Claims Directive Proposal, if it will be approved.

Another important aspect related to the organization of the certification system is that of third-party control by a competent and independent body which, until now, has not always been followed. And, besides of that, the continue monitoring of the operators' compliance. These points are affirmed both by EU Dir. 2024/825 and Green Claims Directive Proposal.

A concrete example of how important these issues are, is the case involving Ali Enterprises in Karachi, Pakistan. The assessment under the certification SA8000 (an international recognized standard for social accountability in the workplace that assesses, among others, the safety of buildings) had just passed, when a fire accident occurred, and many workers lost their lives. In the reality, the company did not have in place an effective system against fire accidents, and the Italian auditors (accredited by Social Accountability International) had subcontracted the auditing to a local organization.

That means that third-party control must not only be serious on paper, but the legislation and its implementation must aim to control the certification system and the continue monitoring, which must be rigorous and effective, across the entire certification relationship. A general critical comment about the actual efficacy of certification systems says that a system of control paid by companies' funds, cannot be successful in protecting workers and will never be successful in that.[88] For this reason, content, organization, controls of the certification systems must be rigorous and effective and operate within a framework of rules established by law.

Another important aspect related to the functioning of certification systems towards greater effectiveness concerns the objective determination of measurable contents in standards and certification systems.[89] Without measurable obligations and output, processes and objectives become empty, intrasparent and ultimately useless. An indirect - even not at all univocal in that sense - provision about this point is that according to which «the requirements for the environmental labelling scheme have been developed by experts that can ensure their scientific robustness» (art. 8, Green Claims Directive Proposal)[90]. Another reference to measurable targets can be found in EU Dir. n. 2024/825 at art. 1.2 *b*), that contain rules to amend art. 6.2 of EU Dir. n.

[88] TE Hoskins, *Il libro della moda anticapitalista*, (It. transl. of *The Anti-Capitalist Book of Fashion*, 1 ed., 2014, Pluto Press) (Il Saggiatore 2024) 148.

[89] For example, standard ISO 9001 has in its structure the point "performance evaluation" that requires a continue monitoring of the company performance. The evaluation process includes internal audit and the monitoring of the performance through KPI key indicators, followed by a review of the overall results to plan any action for improvement. See Podrecca, Sartor (n 64) 16, 23.

[90] The mention of the development by expert is also present in art. 1 of EU Dir. n. 2024/825, that modified art. 2 lett. *r*) of EU Dir. 2005/29.

2005/29 with the addition of lett. *d*), and says that an environmental claim cannot relate to future environmental commitment without «verifiable commitments set out in a detailed and realistic implementation plan that includes measurable and time-bound targets (…)». We can think that sustainability labels, that in line with Recital 7 must be based on a certification scheme, are subject to the same control against unfair commercial practices to which claims are subject (that is the EU Dir. n. 2005/29). Therefore, if the legislator is consistent, in addition to claims and labels, certifications should also be based on measurable obligations, since they concern environmental performance and the related commitments. As other possible reference to measurable objectives, Recital 12 of the Dir. n. 2024/825 about claims based on the offset of greenhouse emissions states that such claims should be only allowed «when they are based on the actual lifecycle impact of the product considered». And Recital 21 of Green Claim Directive Proposal highlights the difficult task of measuring carbon credit offset, referring to the different methodologies, thus demonstrating concern for measurable objectives. Thinking to ISO standards they require the measurement of the performance through indicators similar to KPI (Key Performance Indicator). But they are not homogeneous on this characteristic, because while the ISO 9001 standard is based on performance measurement, the 14001 and 45001 standards see the application of measurability "when possible". Difficulties have been highlighted regarding the measurability of the sustainability metrics in the ESRS standards for sustainability reporting, meaning that the information collected according to these standards is poorly measurable and reliable.[91]

As we saw in the last part of the previous paragraph, the content of certifications, and perhaps even more important, the contents of standards, also need to be radically improved in terms of their alignment with the new sustainability legislation. They must obviously be consistent with existing and future legislation for sustainability goals, and - as they are the most important reference rules in the field - consistent with the UNGPs and the OECD Guidelines.

Indeed, a positive distinguishing feature of standards themselves is their potential global scope, as a global dimension of effectiveness.[92] This is a characteristic that give them a role in supplementing legislation to the benefit of transnational business.[93]

As a final conclusion, standards and certifications are a useful, and – we could say – a concretely necessary tool alongside the law, to pursue the realization of sustainability goals. As seen at par. 1, they are sometimes also referred to by legal provisions, as it is the case with EU Dir. 2024/825 itself which establishes

[91] MC De Cesari, 'Standards di sostenibilità, voto contrario dall'Oic' (Il Sole24ore, 4 december 2025), 40.

[92] Please note that in any case not all standards are global standards, since there are also national and regional standards, as for example the Certified Minas Coffee (CMC) in Brasil, or the national Indonesian Sustainable Palm Oil (ISPO), as in the forest sector there is a tradition of competition between national and international programs as the FSC. National standards could be a first step to the adoption of transnational standards. A Marx and others, 'Global governance through voluntary sustainability standards: Developments, trends and challenges' (2024) 15(4) Global Policy, 716.

[93] As we have seen *supra*, note 34, the areas of business and human rights and environmental sustainability require voluntary standards as a necessary complement to hard form of regulation, «especially since corporate conduct cannot be easily regulated across national borders». About the "smart mix" of legal regulations and private rules, or soft law rules and private standards, Rasche (n 23) 176.

that the use of sustainability labels which are not based on a certification scheme must be prohibited, unless established by a public authority.

Nonetheless, to play this important and necessary role, certification systems are required to turn into a decisive process of improvement, concerning their content, structure (with the provision of measurable objectives), functioning (for example operating through a continue monitoring), assessment process (operating through a third-party assessment) and communication, both in terms of transparency and in terms of the public availability of the content, including that of the underlying standards.

SECTION II

FOCUS PAPERS

Arnone G, 'Smart contracts for Online Dispute Resolution: legal implications and practical applications under EU regulations' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/ejplt251GA

EJPLT
ISSN 2704-8012



Smart Contracts for Online Dispute Resolution: legal implications and practical applications under EU regulations

Gli Smart Contract per la risoluzione online delle controversie: implicazioni giuridiche e applicazioni pratiche alla luce del quadro normativo dell'Unione Europea

GIOIA ARNONE
Postdoctoral Affiliated Researcher
Vrije Universiteit Brussel

Abstract

This paper explores the integration of smart contracts into Online Dispute Resolution (ODR) systems within the EU legal framework. Analysing their potential for automation and transparency in cross-border disputes, it assesses legal gaps, regulatory challenges, and proposes policy recommendations for a harmonised and effective digital justice system in the European Union.

Il presente contributo analizza l'integrazione degli smart contract nei sistemi di risoluzione online delle controversie (ODR) nel quadro giuridico dell'Unione Europea. Esaminando il loro potenziale in termini di automazione e trasparenza nelle controversie transfrontaliere, valuta le lacune normative, le sfide regolatorie e propone raccomandazioni di policy per un sistema di giustizia digitale armonizzato ed efficace nell'Unione Europea.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Smart contracts; Online Dispute Resolution; EU law; Digital justice

Summary: 1. Introduction: The proliferation of digital technologies for legal purposes. – 1.1. Research Objectives and Questions. – 2. Smart Contracts: Definition and Characteristics. – 3. Legal Framework for Smart Contracts in ODR. – 4. Technological Infrastructure and Implementation of Smart Contracts in Online Dispute Resolution (ODR). – 4.1. Blockchain Integration and Regulatory Interplay in ODR. – 5. Practical Implementations of Smart Contracts in ODR Systems. – 6. Ethical Implications of Automating Dispute Resolution. – 7. Conclusions: Final considerations on the effective integration of smart contracts into ODR frameworks.

1. Introduction: The proliferation of digital technologies for legal purposes.

The proliferation of digital technologies continues to transform the landscape of commercial transactions and legal processes. One of the most impactful developments is the rise of Online Dispute Resolution (ODR): a method that uses digital platforms to resolve disputes more efficiently than traditional litigation. Concurrently, smart contracts, which embed contractual terms directly into self-executing code on blockchain platforms, are becoming increasingly prevalent across financial and non-financial sectors. These contracts promise to execute precisely as programmed, minimizing reliance on intermediaries. However, the integration of smart contracts within ODR systems introduces a number of unresolved legal and regulatory challenges. While ODR systems offer an innovative mechanism for pre-judicial resolution of disputes, their application to smart contracts is still relatively underdeveloped. Moreover, existing EU legal instruments lack a cohesive framework to guide their implementation, which hinders both legal certainty and market uptake. Accordingly, this paper seeks to critically examine the interplay between smart contracts and ODR in the context of European Union (EU) regulations, by asking whether and how existing legal frameworks can accommodate blockchain-based contractual enforcement within digital dispute mechanisms.[1]

Alternative Dispute Resolution (ADR) has long been promoted as a faster, more cost-effective substitute for traditional courtroom litigation. In recent decades, technological advancements have given rise to ODR, a digital evolution of ADR conducted partially or entirely online.[2] While ODR offers clear

[1] A Bokolo, 'Deployment of Distributed Ledger and Decentralized Technology for Transition to Smart Industries' (2023) 43 Environment Systems and Decisions 298; DA Zetzsche and others, 'The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy' (2020) ECGI Law Working Paper No 566/2020 <https://ssrn.com/abstract=3725395> accessed 2 September 2025.

[2] D Rainey, MSA Abdel Wahab and E Katsh, *Online Dispute Resolution — Theory and Practice: A Treatise on Technology and Dispute Resolution* (2nd edn, Eleven International Publishing 2021) <https://www.torrossa.com/en/resources/an/5486927> accessed 2 September 2025; EA Onţanu, 'Normalising the Use of Electronic Evidence: Bringing Technology Use into a Familiar Normative Path in Civil Procedure' (2022) 12(3) Oñati Socio-Legal Series 582 <https://doi.org/10.35295/OSLS.IISL/0000-0000-0000-1304> accessed 2 September 2025.

advantages in terms of accessibility and efficiency, it also raises critical concerns regarding party consent, data protection, and procedural fairness. Unlike traditional ADR, ODR lacks face-to-face negotiation, and decisions are often binding regardless of whether the resolution process is facilitated by AI, blockchain, or other technologies.[3]

This paper focuses specifically on the legal implications and practical applications of smart contracts within the ODR framework, with a special emphasis on their compatibility with EU regulations. It thus aims to inform both scholars and policymakers about the regulatory gaps and normative tensions that smart contract integration entails, while exploring technical affordances and their limitations.

1.1. Research Objectives and Questions.

The primary objective of this study is to assess the legal feasibility and practical implementation of smart contracts within the context of ODR systems regulated by the European Union. It aims to explore the compatibility of smart contracts with the ODR Regulation (EU No 524/2013) and the Directive on Consumer ADR (2013/11/EU), and to analyze their potential impact on consumer safety, procedural rights, and economic interests.[4] Thus, the research is structured around the following main question: How can smart contracts be effectively integrated into Online Dispute Resolution (ODR) systems within the European Union in a way that ensures legal enforceability, procedural fairness, and technological robustness?

To address this question, the analysis is guided by the following sub-questions:

- SRQ1: To what extent are current EU legal frameworks equipped to meet the dispute resolution needs arising from smart contracts and cryptocurrency-based transactions?
- SRQ2: How can blockchain-integrated ODR mechanisms be designed to guarantee fairness, enforceability, and compliance with procedural norms in decentralized environments?
- SRQ3: What legal, technological, and regulatory challenges arise from the convergence of smart contracts, ODR, and cryptocurrencies, and how can these be addressed through interdisciplinary approaches?
- SRQ4: What role can AI-driven tools and decentralized arbitration platforms play in enhancing the scalability and trustworthiness of dispute resolution for digital transactions?

[3] LC Voumik and others, 'CO_2 Emissions from Renewable and Non-Renewable Electricity Generation Sources in the G7 Countries: Static and Dynamic Panel Assessment' (2023) 16(3) Energies 1044 <https://doi.org/10.3390/en16031044> accessed 2 September 2025; AJ Schmitz, 'Picking the Proper Technological Tool for Problem-Solving in Arbitration' (2023) SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4608415> accessed 2 September 2025.

[4] A Ferreira, P Sandner, 'EU Search for Regulatory Answers to Crypto Assets and Their Place in the Financial Markets' Infrastructure' (2021) 43 Computer Law & Security Review 105632 <https://doi.org/10.1016/j.clsr.2021.105632> accessed 2 September 2025; S Fiorentino, S Bartolucci, 'Blockchain-Based Smart Contracts as New Governance Tools for the Sharing Economy' (2021) 117 Cities 103325 <https://doi.org/10.1016/j.cities.2021.103325> accessed 2 September 2025.

Together, these sub-questions shape the doctrinal, technological, and normative analysis developed throughout the paper and collectively contribute to answering the main research question.

This research employs a doctrinal legal methodology, supported by illustrative case studies, to analyse the legal and technological dimensions of smart contracts in ODR. The analysis is grounded in a positivist legal approach, with a focus on interpreting existing EU regulations and their application to emerging smart contract models.[5] A black-letter law framework is adopted to evaluate contract law doctrines relevant to smart contracts and to assess their enforceability within digital dispute resolution mechanisms. The geographical scope is limited to EU Member States, focusing on harmonized regulatory instruments such as Regulation No. 910/2014 (eIDAS), which defines trust services relevant to digital identification and authentication.[6] The study also examines how sectoral laws – such as competition law and virtual transaction (VT) law – interface with the enforcement of smart contract-based dispute settlements.

The methodological approach thus enables both the interpretive evaluation of binding legal norms and the functional analysis of emerging digital tools within live or near-live regulatory contexts. Two practical case studies are included to illustrate these dynamics: (1) the judicial review of the AI-based platform Verivox in the context of antitrust proceedings, and (2) the implementation of smart contract arbitration clauses in real estate and digital payment applications.[7]

2. Smart Contracts: Definition and Characteristics.

Online Dispute Resolution (ODR) refers to dispute resolution processes that are conducted, wholly or partially, through digital means (Rainey et al., 2021; Alessa, 2022). Its significance is particularly pronounced in cross-border transactions within the European internal market, where traditional legal processes often struggle with jurisdictional and procedural complexities.[8] EU

[5] J Chaisse, JM Kirkwood, 'Smart Courts, Smart Contracts, and the Future of Online Dispute Resolution' (2022) Stanford Journal of Blockchain Law & Policy <https://stanford-jblp.pubpub.org/> accessed 2 September 2025; H Hamledari, M Fischer, 'Role of Blockchain-Enabled Smart Contracts in Automating Construction Progress Payments' (2021) 13(1) Journal of Legal Affairs and Dispute Resolution in Engineering and Construction <https://doi.org/10.1061/(ASCE)LA.1943-4170.0000442> accessed 2 September 2025; AP Gurgun, K Koc, 'Administrative Risks Challenging the Adoption of Smart Contracts in Construction Projects' (2022) 29(2) Engineering, Construction and Architectural Management 989 <https://doi.org/10.1108/ECAM-09-2020-0678> accessed 2 September 2025.

[6] CP Sempere, 'Crypto Assets and Financial Data Space Regulation in the EU's Hybrid System of Hard and Soft Law' in Governance and Control of Data and Digital Economy in the European Single Market (2025) 71 <https://doi.org/10.1007/978-3-031-74889-9> accessed 2 September 2025; F Bassan, M Rabitti, 'From Smart Legal Contracts to Contracts on Blockchain: An Empirical Investigation' (2024) 55 Computer Law & Security Review 106035 <https://doi.org/10.1016/j.clsr.2024.106035> accessed 2 September 2025.

[7] M Cappai, 'The Role of Private and Public Regulation in the Case Study of Crypto-Assets: The Italian Move Towards Participatory Regulation' (2023) 49 Computer Law & Security Review 105831 <https://doi.org/10.1016/j.clsr.2023.105831> accessed 2 September 2025; F Zatti and others, *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (European Law Institute 2022) <https://www.europeanlawinstitute.eu> accessed 2 September 2025.

[8] DA Zetzsche and others, 'The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy' (2020) ECGI Law Working Paper No 566/2020 <https://ssrn.com/abstract=3725395> accessed 2

consumer protection laws, grounded in *de lege ferenda* considerations, support the development of such digital platforms at the EU level. [9] Consumer protection remains a core value of the EU legal order,[10] while access to justice continues to be predominantly associated with access to courts, despite ongoing debates about the adequacy of this approach in the digital era.[11] ODR platforms have been envisioned as mechanisms to enhance product clarity, accessibility, and legal redress in the digital marketplace. In 2011, the European Commission initiated comprehensive regulatory efforts to establish a standardized ODR framework. This culminated in a web-based platform facilitating the cross-border processing and storage of disputes submitted by ODR providers.

This conceptual grounding lays the foundation for understanding the legal and technological compatibility issues addressed in SRQ1 and SRQ3, while contextualizing the EU's normative commitments to digital justice.

While the principle of party autonomy is well-established in classical contract theory, the use of blockchain-based smart contracts introduces unique challenges related to creation, enforcement, and oversight. Smart contracts, when implemented via distributed ledger technologies (DLTs), often operate without human intermediaries, prompting concerns about their enforceability and compatibility with national legal systems.[12] Legal questions persist: Are such transactions enforceable? Can they comply with public policy or mandatory legal provisions? [13] Originating from Szabo's (1994) conceptualization, smart contracts are defined as "a set of promises, specified

September 2025; J Wagner, 'The European Union's Model of Integrated Border Management: Preventing Transnational Threats, Cross-Border Crime and Irregular Migration in the Context of the EU's Security Policies and Strategies' in Patterns in Border Security (Routledge 2022) 76; M H Zakir, S Ali, 'Cross-Border Trademark Infringement in the Digital Age: Jurisdictional Challenges and Harmonization Efforts' (2023) 3(2) Pakistan Islamicus: An International Journal of Islamic and Social Sciences; K Mania, 'Online Dispute Resolution: The Future of Justice' (2015) 1(1) International Comparative Jurisprudence 76 <https://doi.org/10.1016/j.icj.2015.10.006> accessed 2 September 2025.

[9] S Rudohradská, D Treščáková, 'Proposals for the Digital Markets Act and Digital Services Act: Broader Considerations in Context of Online Platforms' (2021) 5 EU and Comparative Law Issues and Challenges Series (ECLIC) 487 <https://doi.org/10.25234/eclic/18317> accessed 2 September 2025.

[10] J Andraško, M Mesarčík, 'Those Who Shall Be Identified: The Data Protection Aspects of the Legal Framework for Electronic Identification in the European Union' (2021) 11(2) TalTech Journal of European Studies 3 <https://doi.org/10.2478/bjes-2021-0012> accessed 2 September 2025.

[11] JE Teixeira, ATC Tavares-Lehmann, 'Industry 4.0 in the European Union: Policies and National Strategies' (2022) 180 Technological Forecasting and Social Change 121664 <https://doi.org/10.1016/j.techfore.2022.121664> accessed 2 September 2025.

[12] K Ahsan, S Akbar, B Kam, 'Contract Cheating in Higher Education: A Systematic Literature Review and Future Research Agenda' (2022) 47(4) Assessment & Evaluation in Higher Education 523 <https://doi.org/10.1080/02602938.2021.1931660> accessed 2 September 2025; SN Khan and others, 'Blockchain Smart Contracts: Applications, Challenges, and Future Trends' (2021) 14(5) Peer-to-Peer Networking and Applications 2901 <https://doi.org/10.1007/s12083-021-01127-0> accessed 2 September 2025; A Dixit and others, 'Towards User-Centered and Legally Relevant Smart-Contract Development: A Systematic Literature Review' (2022) 26 Journal of Industrial Information Integration 100314 <https://doi.org/10.1016/j.jii.2021.100314> accessed 2 September 2025.

[13] S-Y Lin and others, 'A Survey of Application Research Based on Blockchain Smart Contract' (2022) 28(2) Wireless Networks 635 <https://doi.org/10.1007/s11276-021-02874-x> accessed 2 September 2025; TM Hewa and others, 'Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research' (2021) 9 IEEE Access 87643 <https://doi.org/10.1109/ACCESS.2021.3068178> accessed 2 September 2025; G Zarra, 'Testing the Distinction Between Public Policy and Overriding Mandatory Rules' in *Imperativeness in Private International Law* (TMC Asser Press 2022) 55 <https://doi.org/10.1007/978-94-6265-499-0_2> accessed 2 September 2025.

in digital form, which are self-enforcing through software protocols".[14] These contracts encode rights, obligations, and enforcement mechanisms, thus removing the need for institutional enforcement.[15]

However, for smart contracts to be legally viable, they must include all elements necessary to constitute binding agreements. These include the digital embedding of legal norms, conditions, and enforcement triggers within the code itself. [16] These issues intersect with Research Questions 1 and 3 by underscoring the need for legislative adaptation and technological standardization.

ODR has developed in parallel with the proliferation of internet-based commerce, providing a flexible and efficient alternative to traditional dispute resolution. The earliest documented implementation occurred in 1999 in the U.S., where the Lucas County Court of Common Pleas adopted fully online procedures.[17]

The EU has been particularly proactive in this domain, promoting what has been termed "Regulatory ODR." This involves institutionalizing platforms that facilitate structured dispute resolution between consumers and traders in cross-border e-commerce.

3. Legal Framework for Smart Contracts in ODR.

The European Union has taken a progressive stance on regulating smart contracts and digital services, evidenced by recent proposals for the Digital Services Act and legislation on platform work.[18] Member States are expected to adopt harmonized interpretations of legal ambiguities while implementing national-level provisions consistent with overarching EU goals.[19]

---

[14] P Ortolani, 'Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin' (2016) 36(3) Oxford Journal of Legal Studies 595 <https://ssrn.com/abstract=2730554> accessed 2 September 2025.

[15] A Rawashdeh, 'Bridging the Trust Gap in Financial Reporting: The Impact of Blockchain Technology and Smart Contracts' (2025) 23(2) Journal of Financial Reporting and Accounting 660 <https://doi.org/10.1108/JFRA-08-2023-0494> accessed 2 September 2025; S Secinaro, D Calandra and P Biancone, 'Blockchain, Trust, and Trust Accounting: Can Blockchain Technology Substitute Trust Created by Intermediaries in Trust Accounting? A Theoretical Examination' (2021) 14(2) International Journal of Management Practice 129 <https://doi.org/10.1504/IJMP.2021.113824> accessed 2 September 2025.

[16] V Dwivedi and others, 'A Formal Specification Smart-Contract Language for Legally Binding Decentralized Autonomous Organizations' (2021) 9 IEEE Access 76069 <https://doi.org/10.1109/ACCESS.2021.3081926> accessed 2 September 2025; A Ferreira, P Sandner, 'EU Search for Regulatory Answers to Crypto Assets and Their Place in the Financial Markets' Infrastructure' (2021) 43 Computer Law & Security Review 105632 <https://doi.org/10.1016/j.clsr.2021.105632> accessed 2 September 2025.

[17] E Chioatto, P Sospiro, 'Transition from Waste Management to Circular Economy: The European Union Roadmap' (2023) 25(1) Environment, Development and Sustainability 249 <https://doi.org/10.1007/s10668-021-02050-3> accessed 2 September 2025; E Eckert, O Kovalevska, 'Sustainability in the European Union: Analyzing the Discourse of the European Green Deal' (2021) 14(2) Journal of Risk and Financial Management 80 <https://doi.org/10.3390/jrfm14020080> accessed 2 September 2025; I Ulnicane, 'Artificial Intelligence in the European Union' in *The Routledge Handbook of European Integrations* (Routledge 2022) 254 <https://doi.org/10.4324/9780429262081-19> accessed 2 September 2025.

[18] DA Zetzsche and others, 'DLT-Based Enhancement of Cross-Border Payment Efficiency – A Legal and Regulatory Perspective' (2021) 15(1–2) Law and Financial Markets Review 70 <https://doi.org/10.1080/17521440.2022.2065809> accessed 2 September 2025.

[19] JE Teixeira and ATC Tavares-Lehmann, 'Industry 4.0 in the European Union: Policies and National Strategies' (2022) 180 Technological Forecasting and Social Change 121664 <https://doi.org/10.1016/j.techfore.2022.121664> accessed 2 September 2025; L Battista, 'The European

Despite growing interest, the legal classification of smart contracts remains contested. Some jurisdictions treat them as standard electronic contracts, while others hesitate to grant them full legal standing when implemented on blockchain systems.[20]

Their legal enforceability depends heavily on party choice of law and technical standards that can verify identity and intent—elements currently lacking in uniformity across the EU (Ferreira, 2021). Smart contracts can complement rather than displace traditional legal intermediaries, requiring legislation that accounts for their societal implications.[21]

These ambiguities underscore the need for a harmonized legal ontology of smart contracts within the EU, especially regarding the parameters of digital consent, intent, and enforcement. While the EU is considering separate regulations for automated contracts, key concerns regarding party collaboration, dispute resolution, and enforcement remain inadequately addressed.[22] This section thus contributes to answering SRQ1 and SRQ2, by identifying both the progress and the critical regulatory gaps that hinder the full legal operability of smart contract-enabled ODR systems.

The rise of digital marketplaces has placed pressure on traditional legal mechanisms to offer cost-effective dispute resolution for small claims.[23] EU law currently recognizes multiple avenues for alternative dispute resolution, including statutory mediation and arbitration. Yet, a dichotomy exists between traditional ADR, grounded in legal formalism, and ODR, which increasingly relies on automated, IT-driven processes.[24]

Directives 2013/11/EU and Regulation No. 524/2013 specify required functionalities for compliant ODR systems, but lack deeper normative guidance

---

Framework Agreement on Digitalisation: A Tough Coexistence Within the EU Mosaic of Actions' (2021) 1 Italian Labour Law E-Journal 14 <https://doi.org/10.6092/issn.1561-8048/13357> accessed 2 September 2025.

[20] F Heyman, PJ Norbäck and L Persson, 'Digitalisation, Productivity and Jobs: A European Perspective' in *The European Union and the Technology Shift* (Springer International Publishing 2021) 135–59 <https://doi.org/10.1007/978-3-030-63672-2_6>; I Paweloszek, N Kumar and U Solanki, 'Artificial Intelligence, Digital Technologies and the Future of Law' (2022) Futurity Economics & Law 22–32 <https://doi.org/10.57125/fel.2022.06.25.03>; J Brodny, M Tutak, 'Assessing the Level of Digitalization and Robotization in the Enterprises of the European Union Member States' (2021) 16(7) PLOS ONE e0254993 <https://doi.org/10.1371/journal.pone.0254993>.

[21] M Vatiero, 'Smart Contracts vs Incomplete Contracts: A Transaction Cost Economics Viewpoint' (2022) 46 Computer Law & Security Review 105710 <https://doi.org/10.1016/j.clsr.2022.105710>; D Wiegandt, 'Blockchain and Smart Contracts and the Role of Arbitration' (2022) 39(5) Journal of International Arbitration 671–90 <https://doi.org/10.54648/JOIA2022029>.

[22] AJ Schmitz, 'Picking the Proper Technological Tool for Problem-Solving in Arbitration' (2023) SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4608415>; N Del Sarto, L Gal and F Ielasi, 'Financial Innovation: The Impact of Blockchain Technologies on Financial Intermediaries' (2024) 12(01) Journal of Financial Management, Markets and Institutions <https://doi.org/10.1142/S2282717X23500056>.

[23] ML Chiarella, 'Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment' (2022) 9(1) Athens Journal of Law 33–58 <https://doi.org/10.30958/ajl.9-1-2>; F Lagioia and others, 'AI in Search of Unfairness in Consumer Contracts: The Terms of Service Landscape' (2022) 45(3) Journal of Consumer Policy 481–536 <https://doi.org/10.1007/s10603-022-09520-9>.

[24] B Singh, 'Unleashing Alternative Dispute Resolution (ADR) in Resolving Complex Legal-Technical Issues Arising in Cyberspace Lensing E-Commerce and Intellectual Property: Proliferation of E-Commerce Digital Economy' (2023) 5(10) Revista Brasileira de Alternative Dispute Resolution 81–105 <https://doi.org/10.52028/RBADR.V5I10.ART04.IND>; K Mania, 'Online Dispute Resolution: The Future of Justice' (2015) 1(1) International Comparative Jurisprudence 76–86 <https://doi.org/10.1016/j.icj.2015.10.006>; F Guillaume, S Riva, 'Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice' in *Blockchain and Private International Law* (Brill | Nijhoff 2023) 549-641 <https://doi.org/10.1163/9789004514850_022>.

on fairness, transparency, and accessibility.[25] These instruments provide a foundational basis for integrating smart contracts but remain silent on their code-based logic, enforceability triggers, and compatibility with general principles of consumer protection and procedural justice. For smart contract-enabled ODR platforms to be trustworthy and legally sound, regulators must address governance models, proportional costs, and data protection standards. This reflects SRQ2's focus on ensuring enforceability and procedural fairness in decentralized contexts.

Three major legal challenges persist in the enforceability of smart contracts within the EU:

- Governing Law and Jurisdiction: Determining the applicable law and competent forum remains complex due to the decentralized and borderless nature of blockchain technologies;[26]
- Dispute Resolution Mechanisms: Parties must predefine not only the dispute resolution method but also the jurisdictional authority empowered to enforce outcomes. Traditional criteria may need adaptation to address the decentralized environment;[27]
- Regulatory Compliance: Compliance with AML and counter-terrorism laws is hindered by the pseudonymous nature of blockchain transactions. Regulatory guidance is urgently needed to ensure legal traceability and consumer protection.[28]

These legal concerns directly impact the feasibility of embedding enforceable logic into ODR processes, revealing a need for enhanced legislative adaptation to emerging contractual forms (RQ1 and RQ3). The lack of uniform standards for digital consent, intent verification, and recourse mechanisms continues to inhibit broader adoption of smart contract frameworks in legally significant settings.

4. Technological Infrastructure and Implementation of Smart Contracts in Online Dispute Resolution (ODR).

The implementation of smart contracts within Online Dispute Resolution (ODR) platforms requires a sophisticated and well-supported technological

[25] T da Fonseca Soares, 'Arbitration and Mediation in Consumer Disputes at the Consumer's Option' (2024) 32(2) European Review of Private Law 193–220 <https://doi.org/10.54648/ERPL2024016>; F Casarosa, 'Access to Justice Through Alternative Dispute Resolution Mechanisms: Principles Emerging from the CJEU Jurisprudence' (2024) 3 Opinio Juris in Comparatione 1–23 <https://rm.coe.int/declaration-en/16809ea1e2>.

[26] P Tolmach and others, 'A Survey of Smart Contract Formal Specification and Verification' (2021) 54(7) ACM Computing Surveys (CSUR) 1–38 <https://doi.org/10.1145/3464421>.

[27] TM Hewa and others, 'Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research' (2021) 9 IEEE Access 87643–62 <https://doi.org/10.1109/ACCESS.2021.3068178>; N Kannengiesser and others, 'Challenges and Common Solutions in Smart Contract Development' (2021) 48(11) IEEE Transactions on Software Engineering 4291–318 <https://doi.org/10.1109/TSE.2021.3116808>.

[28] I Zavoli, C King, 'The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis' (2021) 84(4) The Modern Law Review 740–71 <https://doi.org/10.1111/1468-2230.12628>; FMJ Teichmann, 'Current Developments in Money Laundering and Terrorism Financing' (2023) 26(2) Journal of Money Laundering Control 337–48 <https://doi.org/10.1108/JMLC-05-2019-0043>; C Singh, W Lin, 'Can Artificial Intelligence, RegTech and CharityTech Provide Effective Solutions for Anti-Money Laundering and Counter-Terror Financing Initiatives in Charitable Fundraising' (2021) 24(3) Journal of Money Laundering Control 464–82 <https://doi.org/10.1108/JMLC-09-2020-0100>.

infrastructure. Central to this infrastructure is the selection of an appropriate blockchain platform, as each platform offers distinct capabilities, scripting languages, and integration models. For instance, Hyperledger Composer provides a robust, modular framework for permissioned networks with human-readable code, while platforms like Waves support contract development in Scala, and Ethereum enables coding directly within the business logic using Solidity.[29] These variations significantly influence how smart contracts are deployed and operated within ODR systems.

Blockchain-based smart contracts rely on digital wallets—not in the traditional sense, but as graphical user interfaces that enable users to manage identities and tokens (often Ether in Ethereum ecosystems). These interfaces are often supported by JavaScript on the client side and utilize external JSON APIs to fetch real-time data regarding account balances, transaction statuses, and market values.[30] Development tools such as browser-solidity, command-line interfaces (e.g., Geth), and Integrated Development Environments (IDEs) allow for the creation, testing, debugging, and deployment of smart contracts in an interactive and accessible manner.

These contracts are inherently dynamic and programmable. Their self-executing nature enables them to autonomously perform a series of predefined actions once specified conditions are met, significantly reducing the need for third-party enforcement. As such, smart contracts offer both transparency and immutability: two features that are foundational for enhancing trust in digital agreements. Moreover, their deployment within decentralized systems ensures resistance to tampering and provides an auditable trail of actions, facilitating enforceability in legal or quasi-legal frameworks.[31]

This section contributes to SRQ2 and SRQ4 by outlining the technical conditions necessary for smart contract enforceability and evaluating how infrastructure choices – such as platform type and language – impact regulatory compatibility and procedural reliability.

4.1. Blockchain Integration and Regulatory Interplay in ODR.

The convergence of blockchain technology and ODR marks a transformative phase in the legal-tech ecosystem. Originally developed to prevent double spending in cryptocurrencies, blockchain has rapidly evolved into a powerful infrastructure applicable in fields as diverse as digital identity management,

[29] P Sharma, R Jindal, MD Borah, 'A Review of Smart Contract-Based Platforms, Applications, and Challenges' (2023) 26(1) Cluster Computing 395–421 <https://doi.org/10.1007/s10586-021-03491-1>; SY Lin and others, 'A Survey of Application Research Based on Blockchain Smart Contract' (2022) 28(2) Wireless Networks 635–90 <https://doi.org/10.1007/s11276-021-02874-x>;

[30] P Tolmach and others, 'A Survey of Smart Contract Formal Specification and Verification' (2021) 54(7) ACM Computing Surveys (CSUR) 1–38 <https://doi.org/10.1145/3464421>.

[31] J Rosa-Bilbao, J Boubeta-Puig, A Rutle, 'EDALoCo: Enhancing the Accessibility of Blockchains Through a Low-Code Approach to the Development of Event-Driven Applications for Smart Contract Management' (2023) 84 Computer Standards & Interfaces 103676 <https://doi.org/10.1016/j.csi.2022.103676>; H Wu and others, 'On-Site Construction Quality Inspection Using Blockchain and Smart Contracts' (2021) 37(6) Journal of Management in Engineering <https://doi.org/10.1061/(ASCE)ME.1943-5479.0000967>.

asset registration, voting systems, and audit mechanisms.[32] Its intrinsic features – immutability, transparency, decentralization, and distributed consensus – render it a natural fit for implementing automated dispute resolution mechanisms.

In the context of ODR, blockchain serves as a foundation for embedding smart contracts into digital platforms that offer automated or semi-automated mediation and arbitration services. Some platforms integrate these tools in collaboration with regulatory frameworks, such as the EU Regulation on ODR and the EU Crowdfunding Service Providers Regulation. These developments envisage a future where accredited ODR providers can be certified to operate as authorized financial intermediaries, raising capital through tokenized ventures and verifying compliance through blockchain-backed procedures.[33]

Moreover, the regulatory landscape is gradually adapting to these innovations. The European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) are tasked with overseeing these developments, ensuring that smart contract-integrated ODR systems remain aligned with data protection obligations, such as those enshrined in the General Data Protection Regulation (GDPR), and with broader financial service regulations.[34] This regulatory interplay highlights the possibility for blockchain-integrated ODR platforms to evolve within a semi-public, semi-private architecture – responding to the need for trustable, automated legal services articulated in SRQ2 and SRQ4. However, certain contracts – such as those relating to gambling, land sales, financial services, and personal services – remain excluded from smart contract applications due to their complex legal and jurisdictional implications.[35]

5. Practical Implementations of Smart Contracts in ODR Systems.

The deployment of smart contracts within actual ODR settings has been particularly notable in e-commerce environments where transactions often involve standardized, low-value claims. These include disputes over delivery failures, defective goods, or refund policies. Traditional ODR mechanisms in such contexts, as seen with platforms like eBay and PayPal, rely on a combination of conciliation, mediation, and arbitration. The integration of smart contracts into such frameworks enhances efficiency by enabling

[32] A Hassan and others, 'Secured Insurance Framework Using Blockchain and Smart Contract' (2021) Scientific Programming 1–11 <https://doi.org/10.1155/2021/6787406>; D Negi and others, 'Block Chain Platforms and Smart Contracts' in *Blockchain Technology: Concepts and Applications* (Springer 2021) 65–76 <https://doi.org/10.1007/978-3-030-65691-1_5>.

[33] C Cauffman, C Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12(4) European Journal of Risk Regulation 758–74 <https://doi.org/10.1017/err.2021.8>; A Turillazzi and others, 'The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications' (2023) 15(1) Law, Innovation and Technology 83–106 <https://doi.org/10.1080/17579961.2023.2184136>.

[34] M Bakhramovna, 'ODR (Online Dispute Resolution) System as a Modern Conflict Resolution: Necessity and Significance' (2022) 4(3) Journal of Modern Science 443–52

[35] F Amato and others, 'A Model for Verification and Validation of Law Compliance of Smart Contracts in IoT Environment' (2021) 17(11) IEEE Transactions on Industrial Informatics 7752–59 <https://doi.org/10.1109/TII.2021.3057595>; A Ferreira, P Sandner, 'EU Search for Regulatory Answers to Crypto Assets and Their Place in the Financial Markets' Infrastructure' (2021) 43 Computer Law & Security Review 105632 <https://doi.org/10.1016/j.clsr.2021.105632>.

automatic enforcement of outcomes directly tied to pre-agreed conditions in the digital agreement itself.[36] In scenarios where parties have consented in advance to the binding nature of dispute resolutions conducted via ODR systems, the final decisions can carry enforceability comparable to arbitral awards. This dual nature – automation and legal binding effect – makes smart contract-based ODR particularly suited to addressing the "Arbitrary-action-Uncertainty" (AAU) triangle identified in commercial relations, where parties either self-regulate, resort to private arbitration, or invoke public judicial authority.[37]

Despite their growing adoption, smart contracts in ODR remain primarily confined to private initiatives. Public regulatory bodies in Europe have yet to fully embrace their potential for broader legal processes, particularly in high-stakes or non-standard contract categories. [38] Nonetheless, existing frameworks such as the European Small Claims Procedure (ESCP), governed by Regulation (EU) No 861/2007, exemplify the viability of fully online dispute resolution for cross-border consumer claims under €5,000. The ESCP has opened avenues for digital enforcement of contracts arising from cross-border e-commerce, establishing a legal precedent for integrating smart contract technology into public legal systems.[39]

Notably, the success of smart contracts in such settings relies not only on technological robustness but also on the accessibility and clarity of procedures. Challenges persist, especially when national languages and forms create barriers in cross-border disputes. Yet, the growing recognition of smart contracts as viable tools in ODR underscores their potential for improving legal access and reducing friction in digital marketplaces.[40]

These empirical illustrations reinforce the relevance of smart contracts in enhancing access to justice for low-value disputes, thereby offering a real-world response to SRQ2 and SRQ4. They also underscore the importance of usability, multilingual interfaces, and legally mapped logic within ODR platforms as prerequisites for legal accessibility and consumer trust.

---

[36] H Hamledari, M Fischer, 'Role of Blockchain-Enabled Smart Contracts in Automating Construction Progress Payments' (2021) 13(1) Journal of Legal Affairs and Dispute Resolution in Engineering and Construction <https://doi.org/10.1061/(ASCE)LA.1943-4170.0000442>; P Ortolani, 'A Research Agenda for Online Dispute Resolution for DLT Finance' in *A Research Agenda for Financial Law and Regulation* (2025) 237–50 <https://doi.org/10.4337/9781803929996.00019>.

[37] Y Zhao, H Chen, 'Enhancing Access to Digital Justice: Digital Governance of Dispute Resolution and Dispute Prevention in Online Commercial Activities' (2023) <https://doi.org/10.2139/ssrn.4383117>; G Pendel, I Kc Quirk, 'The Evolution and Impact of Online Dispute Resolution: Drivers, Advantages, Challenges, and Future Prospects' (2023) 10(1) BCDR International Arbitration Review 5–22 <https://doi.org/10.54648/BCDR2023012>.

[38] J Kirkwood and J Chaisse, 'Smart Courts, Smart Contracts, and the Future of Online Dispute Resolution' (2022) *Stanford Journal of Blockchain Law & Policy* (SSRN Scholarly Paper ID 4344466) <https://ssrn.com/abstract=4344466>.

[39] R Simaitis, V Vėbraitė, M Markevičiūtė, 'European Small Claims Procedure in the Realm of the Other European Proceedings' (2022) (1) Revista Ítalo-española de Derecho Procesal 123–36 https://doi.org/10.37417/rivitsproc/685; SS Salehi and M Giacalone, 'The Implementation of the European Small Claims Procedure in Belgium' (2021) (10)2 Journal of European Consumer and Market Law 80-84, <https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/10.1/EuCML2021021>.

[40] M Giacalone, I Abignente, SS Salehi, 'Small in Value, Important in Essence: Lessons Learnt from a Decade of Implementing the European Small Claims Procedure in Italy and Belgium' (2021) 17(2) Journal of Private International Law 308–33 <https://doi.org/10.1080/17441048.2021.1953733>.

6. Ethical Implications of Automating Dispute Resolution.

This research has explored the intersection of smart contracts, cryptocurrencies, and online dispute resolution (ODR) systems within the context of EU legal and regulatory frameworks, critically examining the challenges and opportunities emerging from this convergence.

Dispute categories involving individuals with shared ethnic, religious, or socioeconomic profiles may require a degree of tailored procedural treatment to maintain legitimacy and normative sensitivity. However, the pre-coded nature of smart contracts may constrain such flexibility, thereby privileging certain datasets or user expectations over others. Despite the structural integrity promised by blockchain ledgers, disparities in how procedural fairness is experienced may emerge due to rigid adjudication protocols or unequal access to digital infrastructures.[41] Privacy concerns remain central to the ethical debate. Beyond the conventional analysis of individual consent or data exposure, a more holistic evaluation must consider how smart contract systems function within broader socio-technical ecosystems. Participants' trust in these technologies is shaped not only by the interface but by the alignment of systems with societal norms of fairness, accountability, and recourse.[42]

Furthermore, while ODR platforms aim to enhance accessibility, the promise of access to justice can erode quickly if systems lack the safeguards for appealing decisions, verifying accuracy, or ensuring procedural transparency. Mechanisms that allow users to challenge outcomes before impartial authorities must be a baseline requirement – an ethical and legal imperative to preserve democratic legitimacy in digital adjudication.

Smart contracts also play a dual role – not only in enforcing outcomes but in defining the procedural architecture itself. As this paper has explored, particularly in the e-commerce and consumer protection contexts, smart contracts increasingly shape the architecture of dispute resolution by embedding rules and procedural logic within the code itself. Through a normative-legal and conceptual analysis, drawing on both EU regulatory frameworks and comparative international research,[43] this study has demonstrated that while technical advancements offer clarity and automation, they also risk reproducing structural inequalities unless carefully designed and monitored.

As the European Union and other jurisdictions explore legal mechanisms to facilitate smart contract use in e-commerce dispute settings, they must balance

---

[41] WS Admass, YY Munaye, AA Diro, 'Cyber Security: State of the Art, Challenges and Future Directions' (2024) 2 Cyber Security and Applications 100031 <https://doi.org/10.1016/j.csa.2023.100031>; SM Williamson, V Prybutok, 'Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare' (2024) 14(2) Applied Sciences 675 <https://doi.org/10.3390/app14020675>.

[42] JN Chukwunweike and others, 'The Role of Deep Learning in Ensuring Privacy Integrity and Security: Applications in AI-Driven Cybersecurity Solutions' (2024) 23(2) World Journal of Advanced Research and Reviews 1778–90 <https://doi.org/10.30574/wjarr.2024.23.2.2550>.

[43] TH Pranto and others, 'A Blockchain, Smart Contract and Data Mining Based Approach Toward the Betterment of E-Commerce' (2022) 53(5) Cybernetics and Systems 443–67 <https://doi.org/10.1080/01969722.2021.2018545>; A Dixit and others, 'Towards User-Centered and Legally Relevant Smart-Contract Development: A Systematic Literature Review' (2022) 26 Journal of Industrial Information Integration 100314 <https://doi.org/10.1016/j.jii.2021.100314>.

innovation with the preservation of fundamental legal rights. The emphasis must remain on informality and flexibility, yes – but never at the expense of transparency, legal enforceability, and ethical responsibility.

This section responds directly to RQ3 and RQ4, illuminating the ethical tensions that emerge when automating adjudication logic without sufficient oversight, user recourse, or normative transparency. These ethical dilemmas must be systematically addressed through both legal design and institutional review, ensuring alignment between technological efficiency and democratic legitimacy.

7. Conclusions: Final considerations on the effective integration of smart contracts into ODR frameworks.

This study has examined the regulatory, technical, and normative implications of smart contracts within the evolving framework of ODR in the European Union.

Despite their early-stage implementation, smart contracts are increasingly regarded as transformative instruments for automating and enforcing online agreements, particularly in repetitive, low-value, and cross-border disputes.[44] However, they continue to operate within a legal environment that lacks comprehensive oversight, posing significant challenges for harmonization with procedural justice standards. The potential of smart contract platforms – especially within decentralized ecosystems such as e-commerce, distributed energy markets, and collaborative mobility networks – lies in their ability to standardize and automate dispute procedures with minimal reliance on traditional intermediaries. Their scalability and trustworthiness, however, remain contingent upon resolving core questions of legal enforceability, technical integrity, and procedural fairness.[45]

From a legal standpoint, current EU instruments such as the Digital Services Act, the eIDAS Regulation, and the Markets in Crypto-Assets Regulation (MiCA) offer foundational guidance yet remain insufficient in fully accommodating the automated nature and cross-jurisdictional implications of smart contract-based transactions. Particularly in civil law systems, where contractual validity is often subject to formalistic criteria, the enforceability of code-based obligations demands clearer interpretive frameworks and harmonized definitions of consent, offer, and intent. [46] Interoperability with existing enforcement

[44] D Kirli and others, 'Smart Contracts in Energy Systems: A Systematic Review of Fundamental Approaches and Implementations' (2022) 158 Renewable and Sustainable Energy Reviews 112013 <https://doi.org/10.1016/j.rser.2021.112013>; S Fiorentino, S Bartolucci, 'Blockchain-Based Smart Contracts as New Governance Tools for the Sharing Economy' (2021) 117 Cities 103325 <https://doi.org/10.1016/j.cities.2021.103325>.

[45] W van Groesen, P Pauwels, 'Tracking Prefabricated Assets and Compliance Using Quick Response (QR) Codes, Blockchain and Smart Contract Technology' (2022) 141 Automation in Construction 104420 <https://doi.org/10.1016/j.autcon.2022.104420>; H Wu and others, 'On-Site Construction Quality Inspection Using Blockchain and Smart Contracts' (2021) 37(6) Journal of Management in Engineering <https://doi.org/10.1061/(ASCE)ME.1943-5479.0000967>; P Tolmach and others, 'A Survey of Smart Contract Formal Specification and Verification' (2021) 54(7) ACM Computing Surveys (CSUR) 1.

[46] GH Kasap, 'AI Replace Human Arbitrators? Technological Concerns and Legal Implications' (2021) Journal of Dispute Resolution <https://scholarship.law.missouri.edu/jdr/vol2021/iss2/5 https://ssrn.com/abstract=3863136>.

regimes must be enhanced, particularly through improved alignment with electronic identification and trust services. Frameworks under the eIDAS Regulation should support real-time verification and adaptation of identity status, procedural permissions, and contractual relationships.[47] In this regard, a hybrid public-private partnership model may significantly enhance the credibility and adoption of smart contract infrastructures. The introduction of a "legal witness entity" paradigm could function as an institutional intermediary to verify digital identities, manage compliance layers, and foster public confidence.[48] From a fiscal and regulatory perspective, clarification is also needed as to whether blockchain-based smart contracts are to be treated as services, infrastructure, or hybrid systems. This distinction carries significant implications for taxation, liability, and compliance enforcement. Furthermore, the integration of off-chain communications and oracles for external data validation offers a promising avenue to enhance the responsiveness and contextual sensitivity of smart contracts. However, this advancement must be accompanied by robust governance mechanisms to mitigate manipulation risks and preserve the integrity of input data before the execution of smart contractual clauses.[49]

This study also sought to respond to four foundational research questions and proposes the following synthesized findings and reflections:

- On the adequacy of EU legal frameworks (SRQ1): While partial provisions exist, current EU legal instruments are not yet fully equipped to address the dispute resolution needs emerging from smart contracts and cryptocurrency-based interactions. A harmonized, code-aware legal infrastructure is needed to ensure enforceability, legitimacy, and scalability.
- On designing f air and enforceable blockchain-based ODR mechanisms (SRQ2): Ensuring procedural fairness and legal compliance in decentralized systems requires that blockchain-integrated ODR platforms are embedded with legal safeguards – such as transparent rules of engagement, appeal mechanisms, and authenticated identities. The use of eIDAS-compliant identification systems, oracles, and legally mapped smart clauses can bridge the gap between code and law.
- On the legal, regulatory, and technological challenges (SRQ3): The convergence of ODR, smart contracts, and cryptocurrency raises interdisciplinary challenges involving legal uncertainty, technical immutability, and regulatory fragmentation. Addressing these requires

[47] C Timón López, 'The eIDAS2 Regulation: The European Union's Strategic Vision to Regulate a Digital Identity Metasystem under Citizens' Control as a Public Service / El Reglamento eIDAS2: la Visión Estratégica de la Unión Europea para Regular un Metasistema de Identidad Digital bajo el Control del Ciudadano como Servicio Público' (2024) <http://hdl.handle.net/10201/142101>; EA Onţanu, 'Normalising the Use of Electronic Evidence: Bringing Technology Use into a Familiar Normative Path in Civil Procedure' (2022) 12(3) Oñati Socio-Legal Series 582 <https://doi.org/10.35295/OSLS.IISL/0000-0000-0000-1304>.

[48] J Laux, S Wachter, B Mittelstadt, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk' (2024) 18(1) Regulation & Governance 3 <https://doi.org/10.1111/rego.12512>; A Chiappetta, 'Navigating the AI Frontier: European Parliamentary Insights on Bias and Regulation, Preceding the AI Act' (2023) 12(4) Internet Policy Review <https://doi.org/10.14763/2023.4.1733>.

[49] TK Agrawal and others, Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration (2023) 61(5) International Journal of Production Research 1497–1516. <https://doi.org/10.1080/00207543.2022.2039413>.

coordinated regulatory innovation, drawing from both legal practice and software engineering.

- On the role of AI and decentralized arbitration (SRQ4): AI-driven tools and decentralized arbitration platforms offer considerable promise in enhancing the scalability, accessibility, and reliability of digital justice systems. Yet, their success depends on ensuring algorithmic transparency, ethical safeguards, and compatibility with procedural justice principles – particularly in high-volume, low-value transaction contexts such as cross-border e-commerce.[50] Scalability must never come at the expense of democratic oversight and individual rights.

Looking ahead, this research highlights the urgent need for empirical validation of smart contracts in live ODR environments. The proposed experimental model aims to test the efficacy, trustworthiness, and justice-sensitivity of these systems in real-world settings. Such validation is critical not only to refine technological design but also to ensure alignment with fundamental rights, procedural guarantees, and principles of accountability. Future interdisciplinary research should explore:

- the refinement of legal standards for digital enforceability in automated contracts;
- the development of interoperable public-private identity ecosystems;
- the integration of human oversight into algorithmic dispute resolution processes;
- the impact of legal design and user experience on access to digital justice; and
- the implementation of AI-powered technologies for ODR's triage, prediction, and result assessment processes.

In conclusion, the findings of this study suggest that the effective integration of smart contracts into ODR frameworks must go beyond technological sophistication. It must be grounded in legal certainty, ethical foresight, and procedural legitimacy. Only through such a multidimensional approach can the EU - and other jurisdictions - ensure that technology serves not merely efficiency, but justice itself.

[50] AJ Schmitz, 'Picking the Proper Technological Tool for Problem-Solving in Arbitration' (2023) SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4608415>; BE Howell, PH Potgieter, 'Uncertainty and Dispute Resolution for Blockchain and Smart Contract Institutions' (2021) 17(4) Journal of Institutional Economics 545 <https://doi.org/10.1017/S1744137421000138>; O Elias Oluwafemi and others, 'The Evolution of Green Fintech: Leveraging AI and IoT for Sustainable Financial Services and Smart Contract Implementation' (2024) 23(1) World Journal of Advanced Research and Reviews 2710 <https://doi.org/10.30574/wjarr.2024.23.1.2272>.

Battaglino G, 'The Kleinberg epistemic paradox within contractual discrimination' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252GB

EJPLT
ISSN 2704-8012



The Kleinberg epistemic paradox within contractual discrimination

Il paradosso epistemico di Kleinberg e la discriminazione contrattuale

GIOVANNI BATTAGLINO
PhD candidate
University of Camerino
LAST-JD PhD Candidate
Vrije Universiteit Brussel

Abstract

This paper examines contractual discrimination in the age of Artificial Intelligence through the epistemic paradox formulated by Jon Kleinberg. While the principle of non-discrimination is firmly recognised in European private law, its assessment remains epistemically complex, especially where intent is obscured by human bias or algorithmic processes. Two interpretative models are considered: the formalist, which confines protection to statutory indices and categories, and the substantive-functional, which evaluates discrimination retrospectively and contextually. The paper endorses the latter, showing that Kleinberg's paradox offers limited utility in such a framework, yet regains relevance for formalist approaches. Through doctrinal, legislative, and jurisprudential analysis, reinforced by hypothetical examples, the argument highlights how AI systems may serve as "moral mentors," exposing fractures in a positivist system dominated by binarisation, confinement, and market interests. Ultimately, the interpreter, not legislation alone, must ensure that remedies evolve with the complexity of technological and economic development, safeguarding human dignity.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Il presente contributo esamina la discriminazione contrattuale nell'era dell'Intelligenza Artificiale alla luce del paradosso epistemico formulato da Jon Kleinberg. Sebbene il principio di non discriminazione sia saldamente riconosciuto nel diritto privato europeo, il suo accertamento rimane epistemicamente complesso, specialmente quando l'intento è oscurato da bias umani o da processi algoritmici. Sono presi in considerazione due modelli interpretativi: quello formalista, che circoscrive la tutela agli indici e alle categorie previsti dalla legge, e quello sostanziale-funzionale, che valuta la discriminazione in modo retrospettivo e contestuale. Il contributo aderisce a quest'ultimo, mostrando come il paradosso di Kleinberg offra un'utilità limitata in tale prospettiva, ma riacquisti rilevanza negli approcci formalisti.
Attraverso un'analisi dottrinale, legislativa e giurisprudenziale, corroborata da esempi ipotetici, l'argomentazione evidenzia come i sistemi di Intelligenza Artificiale possano fungere da "mentori morali", mettendo in luce le fratture di un sistema positivistico dominato da binarizzazione, confinamento e interessi di mercato. In ultima analisi, spetta all'interprete e non alla sola legislazione garantire che i rimedi si evolvano in sintonia con la complessità dello sviluppo tecnologico ed economico, salvaguardando la dignità umana.

Keywords: contractual discrimination; artificial intelligence; epistemology; moral mentor; Jon Kleinberg

Summary: 1. Introduction: AI and contractual discrimination within Jon Kleinberg's paradox. – 2. How Discriminatory Treatment Is Evaluated. – 3. *(Follow)* The Reasonable Approach to the Evaluation of Discriminatory Treatment. – 4. Justification of the Alleged Discriminatory Choice and Epistemic Centrality. – 5. Conclusions: The Old Problems of Technique and Liberal Rhetoric in the field of Contractual Liability. The Machine as Moral Mentor and a Revival of Kleinberg's Thesis.

1. AI and contractual discrimination within Jon Kleinberg's paradox.

The use of Artificial Intelligence in contractual relationships raises concerns regarding potential discrimination.[1]

[1] Indeed, the assumption of machine neutrality is now widely contested. AI systems not only replicate but may also amplify the biases embedded in human behavior and social structures. See, for example, part of the legal scholarship specifically addressing algorithmic systems that have demonstrated discriminatory effects: E Falletti, *Discriminazione algoritmica. Una prospettiva* comparata (Giappichelli 2022) 220-229; PM Law and others, 'The Impact of Presentation Style on Human–In–The–Loop Detection of Algorithmic Bias' [2020] GI, arXiv.2004.12388; E Oosterloo, GV Schie, 'The politics and Biases of the "Crime Anticipation System" of the Dutch Police' [2020] Bias Inf. Algorithms Syst.; A Završnik, 'Criminal justice, artificial intelligence systems, and human rights' (2020) 20 (4) Era Forum 567; E Tristram Albert, 'AI in talent acquisition: A review of AI applications used in recruitment and selection' (2019) 18 (5) SHR 215; R Berk and others, 'A convex framework for fair regression' [2017], arXiv:1706.02409.

Non-discrimination is recognised as both a foundational principle and a legal value;[2] nevertheless, its practical assessment remains contested and epistemically complex.[3]

This paper does not address the philosophical or etymological roots of discrimination, nor its conceptual links to human dignity, vulnerability, or equality.[4]

The focus will be on the *ex-post* evaluation of presumed contractual discrimination[5] mediated[6] by a Large Language Models (LLMs).[7]

---

[2] Despite the breadth and fragmented nature of the relevant legal sources, and notwithstanding the existence of general treaties provisions that directly or indirectly address discrimination, the Court of Justice of the European Union has affirmed the principle of non-discrimination as grounded in the principle of equality and as a cornerstone of EU law. On this point, see Court of Justice of the European Communities, Case C-13/94, *P v S and Cornwall County Council*, 30 April 1996 (ECLI:EU:C:1996:170); Court of Justice of European Union, Case C-144/04, *Mangold v Helm*, 22 November 2005 (ECLI:EU:C:2005:709). In other cases, however, the Court of Justice has interpreted the principle of non-discrimination as symbiotic with the principle of human dignity: Court of Justice of the European Communities, Case C-152/82, *Forcheri v Belgian State*, 13 July 1983 (ECLI:EU:C:1983:217); Court of Justice of the European Union, Case C-36/02, *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn*, 14 October 2004 (ECLI:EU:C:2004:614); Case C-144/04 *Werner Mangold v Rüdiger Helm* [2005] ECR I-9981 For scholarly contributions that acknowledge the principle of non-discrimination, see *infra* note 4; for the more specific normative framework concerning contractual matters, see Section 2 below.

[3] On this point, see Sections 2 and following.

[4] For a discussion of the etymology of discrimination, see PS Shin, 'Is There a Unitary Concept of Discrimination?', in D. Hellman, S. Moreau (eds.), *Philosophical foundation of discrimination Law* (Oxford University Press 2013) 161; L Halldenius, 'Dissecting Discrimination' (2005) 14(4) Camb., Q. Healthc. Ethics, 455. For the philosophical foundations of discrimination law, see E Consiglio, *Che cos'è la Discriminazione? Un'introduzione teorica al diritto antidiscriminatorio* (Giappichelli 2020), 131 ff., see also the related bibliography cited therein. In contrast, for a different legal grounding of discrimination in the context of contract law: C Nardocci, 'Artificial Intelligence-based Discrimination: Theoretical and Normative Responses. Perspectives from Europe' (2023) 3 DPCE Online 2385; P Femia, 'Discriminazione (divieto di)', *Enciclopedia del Diritto – I Tematici, Contratto* (Giuffrè Francis Lefebvre 2021) 499 ff.; H Steege, 'Algorithm-Based Discrimination by Using Artificial Intelligence: Comparative Legal Considerations and Relevant Areas of Application' (2021) 1 EJPLT 56; FJ Zuiderveen Borgesius, 'Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence' (2020) 24(10) Int. J. Hum. Rights. 1572; HH Harvey, 'Justifying the Efficacy of Contract Discrimination' (2019) 2 J. Law Innov., 47; M Ciancimino, 'La discriminazione contrattuale: profili rilevanti per la tutela della persona. Note a margine di un recente dibattito dottrinale' (2018) 2 Dir fam. Pers. 668; G Carapezza Figlia, 'Il divieto di discriminazione quale limite all'autonomia contrattuale' (2015) 6 Riv. dir. civ. 1387; D Maffeis, 'Il diritto contrattuale antidiscriminatorio nelle indagini dottrinali recenti' (2015) 1 N. leg. civ comm. 161; L Gentili, 'Il principio di non discriminazione nei rapporti civili' (2009) 2 Riv. crit. dir. priv. 207; AS Vandenberghe, 'The Economics of the Non-Discrimination Principle in General Contract Law' (2007) 4(3) ERCL 411; J Neuner, 'Protection Against Discrimination in European Contract Law' (2006) 1 ERCL 36.

[5] In addition, the notion of discrimination is consistently construed in a strictly negative and legally adverse sense: FJ Zuiderveen Borgesius, 'Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence' (2020) The International Journal of Guman Rights 1573.

[6] The term "mediated" is used here, on the one hand, to reflect a materialistic and human-centered view of technology, beyond any metaphysic speculation. On the other hand, once the assumption of algorithmic neutrality is deconstructed, a factual equivalence emerges between human and machine-generated discriminatory effects. This leads to a behavioristic perspective, whereby the machine may operate as a discriminatory agent in the same way as a human. On this basis, the legal evaluation of discriminatory treatment remains inherently open and subject to diverse interpretations. For further discussion of the relationship between neutrality, agency, and the interaction between technology and law, as well as for the relevant bibliography, see: G Battaglino, 'La fairness algoritmica: incontro tra sviluppo socio–tecnologico ed esigenze dell'ermeneutica giuridica', (2025) 1 B.L. Journal 633-639.

[7] For a comprehensive overview of the general properties of large language models, see WX Zhao and others, 'A Survey of Large Language Models' [2023], arXiv:2303.18223. In this paper, a *summa divisio* is drawn between formal systems and stochastic systems (such as Large Language Models). Consistent with the principle of precision for readability, the analysis does not aim to conceptualise or technically reconstruct these systems from an informatics perspective. Rather, it seeks to clarify their practical legal relevance and operational use within juridical evaluation: Zuiderveen Borgesius (n 4) 1574.

Within the scholarship on algorithmic discrimination, a provocative thesis is advanced by computer scientist Jon Kleinberg.[8] He argues that algorithms, rather than merely obscuring discriminatory behaviour, may assist in its legal evaluation.

The difficulty, he suggests, is epistemic:[9] legal interpreters often struggle to identify intent behind a discriminatory outcome, whether it arises from human implicit bias or from algorithmic processes: while human decision-making is subject to cognitive opacity,[10] algorithms may offer a form of computational transparency.[11] Kleinberg thus poses a provocation: when assessing discriminatory outcomes, are legal interpreter equipped to interrogate deeply hidden cognitive states, or to navigate computational processes?[12]

Against this backdrop, this paper examines the potential of Kleinberg's epistemic paradox as a meaningful analytical tool for understanding and evaluating AI-mediated contractual discrimination?[13]

The analysis begins by establishing how discriminatory treatment is evaluated.[14] From this legal scaffolding, the paper builds two conceptual models through which the legal evaluation of discrimination is commonly articulated: one grounded in legal formalism, the other in substantive functionalism. Both frameworks acknowledge the epistemic difficulty involved in assessing discriminatory outcomes.[15]

The analysis now turns to a critical evaluation of their explanatory power and normative coherence: the paper supports the second approach, the substantive-functional model.[16]

---

[8] J Kleinberg and others, 'Discrimination in the Age of Algorithms' (2019) 10 J. Leg. Anal 113 ff.

[9] In this paper, the term "epistemology" is used, regardless of any broader interpretations, to refer specifically to the capacity to make a legal choice intelligible and understandable to the human subject who is expected to evaluate it, an aspect that remains crucial regardless of the nature of the agent making the decision: P Moro, 'Algoritmi e pensiero giuridico. Antinomie e interazioni' (2019) 2 Media Laws 20-22.

[10] In fact, individuals may lie, dissemble, or be unaware of their own biases. On this sense, see Consiglio (n 4) 84-86.

[11] J Kleinberg (n 7) 116: «Deciding whether there has been discrimination is difficult for one obvious and one less obvious reason. The obvious reason is generic to any legal system: people dissemble, obfuscate, and lie. The less obvious reason is that people may not even know themselves. A large body of research from behavioural science (...) tells us that people themselves may not know why and how they are choosing – even (or perhaps especially) when they think that they do».

[12] ibid, 116: «The opacity of the algorithm does not prevent us from scrutinizing its construction or experimenting with its behaviour, two activities that are impossible with humans. (…) In contrast, a well-regulated process involving algorithms stands out for its transparency and specificity: it is not obscured by the same haze of ambiguity that obfuscates human decision-making. (...) In a nutshell: For the legal system, discovering "on what basis are they choosing?" and "why did they pick those factors?" becomes much more feasible». Accordingly, in the first case (discrimination caused by a human agent), the epistemic problem is rooted in human ontology; in the second (discrimination caused by a machine), the epistemic problem is systemic and operational in nature. In this sense, see: G Gometz, 'Intelligenza artificiale, profilazione e nuove forme di discriminazione' (2019), in F. Mancuso, V. Giordano (eds.), *Ombre del diritto, Materiali dei seminari el Prin 2017, The Dark Side of Law',* 1 ff.

[13] In order to assess the relevance of Kleinberg's epistemic paradox to the legal evaluation of contractual discrimination, this paper adopts a facet recommendatory methodology, which involves distinct descriptive and evaluative phases: L Kestemont, *Handbook on Legal Methodology: From Objective to Method* (Intersentia 2018) 63-73.

[14] On this point, see section 2, which focuses on the EU and Italian normative framework and the relevant scholarship that explicitly engage with the discriminatory contractual wrongdoing.

[15] See infra, section 4.

[16] See infra, Section 3, which focuses through a combination of historical, doctrinal, jurisprudential and logical reasoning.

In this light, Kleinberg's paradox offers limited analytical utility within a substantive-functional evaluation of contractual discrimination.[17]

However, in interpretive practices the paradox regains significance for a more formalistic interpreter. In this sense, the paper expects to propose the machine as a moral mentor, capable of guiding legal interpretation beyond rigid formalism in the evaluation of contractual discrimination. [18]

2. How Discriminatory Treatment Is Evaluated.

To establish the epistemic centrality of evaluating discriminatory conduct, it is necessary to outline when and how the legal system recognises it.

Legislation[19] tend to evaluate discriminatory conduct on the basis of three core indicators:[20] (a) the existence of a detrimental or unfavourable treatment, broadly construed, suffered by an individual or a group; (b) the presence of a protected characteristic, as defined by law, that causally underpins such treatment; (c) the absence of a reasonable justification. [21]

What matters at this stage is to understand how the first two elements, symptomatic indicators of discrimination, are weighed in the legal evaluation.

On this point, it is possible to outline two main interpretative approaches:[22]

---

[17] See infra, Section 4.

[18] See infra, Section 5.

[19] The legislative acts, although the legislator does not possess absolute semantic authority, and language alone is not the sole object of legal science, inevitably serves as a starting point in the reconstruction and interpretation of the legal system. On this point, see P Femia, *Interessi e conflitti culturali nell'autonomia privata e nella responsabilità civile* (Jovene 1990) 11–12, 20–23; P Perlingieri, 'Produzione scientifica e realtà pratica: una frattura da evitare' (1969) 9 Riv. dir. comm. 457–458. Therefore, it must be questioned whether statutory provisions alone can exhaustively define the indicators and criteria required both to assess the discriminatory nature of a given conduct and to attribute legal responsibility for it. on this point see specifically par 3

[20] On this point, with particular reference to elements (a) and (b) identified above, see Article 2 of Directive 2000/43/EC, Directive 2000/113/EC, and Article 43 of the Testo Unico sull'Immigrazione (d. lgs. 25 luglio 1998, n. 286 The first directive seeks to prohibit all forms of discrimination based on race or ethnic origin, particularly in the context of employment (see Article 3, Dir 2000/43/EC). The second addresses discrimination based on sex in the access to and supply of goods and services (see Article 3, Dir 2000/113/EC). The third provision (Article 43) targets discrimination grounded in race, colour, descent, or national or ethnic origin, as well as religious beliefs and practices, regarding the equal enjoyment or exercise of human rights and fundamental freedoms in political, economic, social, and cultural life, as well as in all other areas of public life. Regarding point (c), reference should be made to Article 2(2)(b) of both Directives, which address the concept of indirect discrimination (on which, see infra). Under these provisions, a difference in treatment does not constitute unlawful discrimination if it is objectively justified by a legitimate aim, and if the means of achieving that aim are appropriate and necessary. Both Directive 2000/43/EC and Directive 2000/113/EC have been duly and comprehensively transposed into the domestic legal systems of all EU Member States. In Italy, the implementation of Directive 2000/43/EC was carried out primarily through Legislative Decree No 215 of 9 July 2003, which also established the National Office Against Racial Discrimination (UNAR). Directive 2000/113/EC was implemented by Legislative Decree No 196 of 11 April 2006, which introduced specific provisions ensuring gender equality in access to goods and services. See: Decreto Legislativo 9 luglio 2003, n. 215, Attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica, G.U. n. 173 del 28 luglio 2003; Decreto Legislativo 11 aprile 2006, n. 196, Attuazione della direttiva 2000/113/CE sulla parità di trattamento tra uomini e donne nell'accesso a beni e servizi, G.U. n. 115 del 19 maggio 2006.

[21] The latter element functions as an epistemic exception clause and, as such, its centrality will be addressed in the fourth section.

[22] These models do not reflect rigid doctrinal traditions or established academic labels; rather, they are proposed here as analytical constructs adopted for explanatory clarity and operational effectiveness.

(1) Formalist-legistic:[23] These positions presuppose that the express identification of legal indicators and protected categories is a necessary condition for qualifying a given conduct as discriminatory: when the conduct falls squarely within these predefined legal classifications can the legal status of the affected individual be recognised and protected.

(2) Substantive-functional:[24] under this model, discrimination is understood as a multifactorial phenomenon. Legal Indicators serve as symptomatic markers but are not exhaustive determinants. The evaluation, therefore, goes beyond formal classification and considers the broader structural and contextual effects of the conduct.

3. (Follow) The Reasonable Approach to the Evaluation of Discriminatory Treatment.

Before establishing the epistemic centrality (point c) common to both models, it is necessary to clarify why the substantive-functional approach is preferred. The reasons can be summarised as follows:

(a) Historical contingency**.** Protected indices and categories are context-dependent and evolve over time; they cannot be treated as fixed or exhaustive.[25]

(b) Methodological shortcomings**.** Recognising legal positions solely on statutory signifiers ignores the concrete circumstances of cases and the interests at stake.[26] Rigid reliance on such signifiers risks a tyrannical close of value[27], whereby dominant majorities or stronger contracting parties dictate the framework.[28]

---

[23] Thus, for example, the evaluation of discriminatory conduct is often framed through a twofold analytical distinction based on intersecting dimensions: direct versus indirect discrimination, and intentional versus unintentional discrimination. The first of these distinctions appears to be expressly reflected in Article 2(2) of both Directives previously mentioned, which codify the differentiation between direct and indirect forms of discrimination. On this pint see, Steege (n 4) 60-61. The main distinction between direct and indirect discrimination lies, in fact, in the requirement to establish intentionality in the latter in order for it to o be ascribed legal responsibility. On this point, see: Zuiderveen Borgesius (n 4) 1576-1578. Appears to align with this approach, both in the inquiry into intentionality and in the assessment of a causal nexus between the conduct and the harm, Nardocci (n 4) 2367 ff. The assessment of discrimination as either direct or indirect appears to find a terminological counterpart overseas in the so-called *disparate treatment* and *disparate impact*. On this point, see Kleinberg (n 9) 6-9.

[24] On this approach, see, among others, but most notably Femia (n 4) 498 ff.

[25] Indeed, even prior to the enactment of specific anti-discrimination legislation, racial hatred, religiously motivated sexism, and homophobia were already regarded as morally reprehensible and socially intolerable. This highlights that the very indefinability and fluidity of the legal indicators is not a limitation but rather an integral feature of the concept of discrimination itself. On this point, see Femia (n 4) 505-521; Zuiderveen Borgesius (n 4) 1584-1586; R Post, 'Prejudicial Appearances: The Logic of American Antidiscrimination Law' (2000) 88 Cal L Rev 1, 8–9; F Bagenstos, '"Rational Discrimination," Accommodation, and the Politics of (Disability) Civil Rights' (2003) 89 Va L Rev 825, 846–47. On this point, see Cons. Stato 9 gennaio 2017 n. 30, in *Foroplus.it*

[26] P Perlingieri, 'Relazione conclusiva', in P Perlingieri and L Ruggeri (eds), *Diritto privato comunitario*, II (2nd ESI 2008) 393–399;

[27] On the theory of the "tyrannical value" and its implications for legal methodology and interpretation, see especially Battaglino (n 6) 645-649., along with the bibliography cited therein.

[28] P Femia, 'Segni di valore' [2014] in www.*Civilistica.com*; P Perlingieri, 'Valori normativi e loro gerarchia: una precisazione dovuta a Natalino Irti' [1985] Rass. dir. civ. 298. The very idea of democracy is founded on a compromise which never crystallises into value absolutism. No single value can be elevated to an absolute; instead, it necessarily presupposes the coexistence of diverse opinions and interests, all of which must be

(c) Instrumental nature of indices. Legal indicators are tools, not ends; their application in practice determines whether treatment is discriminatory, justified[29], or belongs "merely" to the domain of morality[30].

On those bases, the second approach appears preferable: discrimination must be understood as a retrospective and complex phenomenon, dependent on circumstances, competing interests, and justifications. The ideological risk, rather than the technical one, is that of a corrupted egalitarianism in which every need becomes a legal entitlement.[31] However, by the same token, denying protection outright simply because the relevant index or category is not represented in a statutory rule or contract[32] would be equally untenable.[33]

In conclusion, indices remain no more than indicators: useful to the interpreter, but not sufficient to exhaust the evaluative task. Rather, the inquiry necessarily shifts from an abstract (and presumptively neutral) assessment to one that is retrospective and concrete.[34]

---

considered. See also H Kelsen, *I fondamenti della democrazia* (Il Mulino 1966) 168–170; F. Rimoli, 'Laicità', in *Enciclopedia Giuridica Treccani* (XVIII, 1990) 8–9.

[29] The criterion, in itself, is always neutral; indeed, more often than not, as in the case of so-called positive discrimination, it is the legal norm itself which requires reliance on that criterion in specific circumstances, without thereby producing an effect that can structurally be regarded as discriminatory. On this point, see D Maffeis, 'Libertà contrattuale e divieto di discriminazione' (2008) 1 Riv. trim. dir. proc. Civ. 425-426.

[30] In certain contexts, however, the use of artificial intelligence systems, similar to those employed in dating platforms such as Tinder, falls outside the scope of legal scrutiny regarding discrimination. For all its sadness, if a woman rejects a man because an AI-based matching system highlights that he is "too short" or "too thin", such a decision remains an expression of personal and affective choice. As such, it is not amenable to judicial review under anti-discrimination law, since the sphere of intimate and emotional preferences is generally regarded as lying beyond the reach of legal regulation. This example is inspired by J Gardner, 'On the Ground of Her Sex(uality) (1998) 18 OJLS 167 ff.

[31] D Maffeis (n 27) 409. Part of the legal scholarship, in order to avoid such an egalitarian drift, where the prohibition of discrimination would unduly restrict contractual freedom, argues that the former should apply only in cases involving a public offer, and not to negotiations between private parties. Although this view is not endorsed here, it may nonetheless be observed that, in the situations under discussion, even if one is not technically faced with a public offer, those who employ LLMs in legally relevant decision-making are invariably enterprises. This lends to the thesis of discrimination advanced here a kind of elliptical value. For the approach that is not endorsed here, see D Maffeis (n 4) 163 ff. By contrast, see Ciancimino (n 4) 678-677.

[32] In this sense, discrimination must be addressed with every instrument that civil law makes available, and not solely through legislative or political mechanisms, as a more positivistic strand of legal scholarship would suggest. This line of reasoning also emphasises the absence of an explicit prohibition against discrimination on the basis of artificial intelligence, a lacuna which could pose a problem at the legislative level. It is as if AI were not regarded as an *instrumentum* that merely mediates and amplifies discriminatory dynamics already present, rather than constituting an autonomous ground of discrimination in itself: Nardocci (n 4) 2367 ff. On this point, moreover, the very criteria themselves, as has already been argued, are historically contingent and carry different weight, at least insofar as their legislative translation is concerned. Thus, for example, while history has led to the enactment of explicit statutory protections against discrimination on the grounds of race or sex, it is also clear that, aside from any personal considerations, the list of protected characteristics may evolve to include new categories (such as LGBT rights). Conversely, other potential indices are excluded precisely because they are not regarded as "appropriate" or "normal". Yet this does not preclude the possibility that, in a given case, reliance on such criteria may still reveal a discriminatory treatment: Shin (n 4) 11-15.

[33] On this point, see Femia (n 4) 517; B Parenzo, 'Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA' (2023) 1 Tecn. Dir. 114.

[34] Moreover, it remains unclear why, if indices and classes are assumed to be all-encompassing of every possible form of discriminatory treatment, thus generating a kind of seriality of discriminatory phenomena, there should be any need to employ an LLM-based system or, more generally, a framework that goes beyond mere formal logic, as if it were itself a formal system. This is particularly evident when considering the availability of formal, interpretable and explainable algorithms, which can already provide a structured and transparent assessment without the epistemic opacity inherent in large-scale machine learning models. On this point, see Battaglino (n 6) 854-856.

4. Justification of the Alleged Discriminatory Choice and Epistemic Centrality.

It is now necessary to turn to point (c) of the framework outlined above: the absence of justification for discriminatory treatment. This element concerns less the structure of evaluation than the attribution of responsibility to an agent. Indeed, even where statutory indices or protected categories are expressly violated in the concrete case, an additional stage of inquiry into the existence of a discriminatory intent (so called: *animus discriminandi*) is often invoked in order to impute the discriminatory treatment to a specific subject. It is precisely here that Kleinberg's epistemic paradox becomes relevant, since the difficulty lies in uncovering the motives behind discrimination.[35]

As noted, para. 1, both human agents and machines, with their different cognitive properties, may conceal the underlying causes or "reasons" for the alleged discriminatory treatment, making evaluation particularly difficult. [36] This epistemic deficit may translate in civil law into a form of de-responsibilisation of the discriminating agent, whether the act is performed directly or mediated by an LLM. In this sense, where discrimination is carried out directly by a human agent, one might conclude that the absence of *intent* to discriminate leads to a finding of no fault. Conversely, in the case of an LLM-based system, the discriminating agent may invoke the machine's autonomy in order to evade liability, thereby appealing to a logic of the kind: "It was not I, but the machine; it discriminated (it is at fault, or in any case endowed with an autonomy that renders me blameless); I merely switched it on." [37] In both cases, therefore, what emerges is a dissimulation of the discriminatory treatment.

In this sense, Kleinberg's proposal proves to be highly attractive, as it may appear preferable to focus on operational capacity rather than on the ontology of the human mind and consciousness (see para. 1). Nevertheless, when transposed into the field of civil law, such a conclusion requires argumentative refinements. Indeed, if, as widely recognised in doctrine, case law, and even within legislation itself, there is no necessary correlation between intentionality and agency for the juridical attribution of a discriminatory effect. [38]

---

[35] On what is meant by the term *epistemic* in the present discussion, see n. 9.

[36] If the discriminatory cause or motive is attributable to a human agent, its concealment (whether conscious or unconscious) remains hidden *in interiore hominis*. By contrast, when it derives from a machine, presupposing the absence of consciousness, the hateful motive is not concealed (the machine does not hate); rather, what remains obscured is the justification of the decision, which is veiled by the system's own technical and operational complexity. In both phenomena, therefore, the "smoking gun" is absent when it comes to assessing the justification of the discriminatory treatment: J Kleinberg, 'Discrimination' (n 9), 27.

[37] On this point, see P. Femia, 'Essere norma. Tesi sulla giuridicità del pensiero macchinico', in P Perlingieri, S Giova, I Prisco (ed.), *Il trattamento algoritmico dei dati tra etica, diritto ed economia* (Esi, 2020), 69.

[38] More generally, civil liability has long since moved beyond the consideration of the agent's intention for the purpose of attributing responsibility under civil law. Intention remains a cornerstone only within the domains of criminal law and/or ethics (C. Maiorca, voce *Responsabilità (teoria gen.)*, in *Enciclopedia del diritto* (XVIII, 1990) 8–9. On this point, the bibliography is vast; it suffices here to refer to those texts that address discrimination directly and which do not treat intention as a necessary condition for attribution: Parenzo (n 27) 105; Zuiderveen Borgesius (n 4) 1573-1574; Shin (n 4) 28; Femia (n 4) 503-504; Harvey (n 4) 55.
On the overcoming of intention as a requirement for the attribution of civil liability, and its relegation to the domain of criminal law, see: Cass. Civ., 21 December 2003, n 46783, C-188/15 *Asma Bougnaoui and Association de défense des droits de l'homme (ADDH) v Micropole SA* (Grand Chamber, 14 March 2017) ECLI:EU:C:2017:204. For further bibliography on this point, see Battaglino (n 6) 645-649.

On this view, Kleinberg's paradox risks losing practical utility, since legal evaluation must ultimately focus on the concrete effects of discrimination rather than the motives behind it.[39]

5. The Old Problems of Technique and Liberal Rhetoric in the field of Contractual Liability. The Machine as Moral Mentor and a Revival of Kleinberg's Thesis.

Following the substantive-functional approach, which conceives indices and categories as multifactorial and does not require intentionality for the attribution of responsibility, Kleinberg's thesis may appear of limited appeal. Nevertheless, part of doctrine and case law still favours a formalist perspective, where both a precise index and a clearly defined class are required to structure a claim, often with an undue emphasis on the actor's intent (illicit motivation).[40] In this sense, Kleinberg notes that human agents tend to conceal unlawful motives behind formal compliance, whereas machines, unburdened by fear of sanctions, may within their operational complexity «reveal our own biases».[41]

His provocation should not be read in absolute terms, but as a conceptual tool to expose formalistic dynamics. Reframed substantively, it frees the interpreter from strict reliance on indices and categories or on the supposed necessity of intentionality.[42]

To illustrate: suppose a hypothetical example where a recruiter refuses to hire a candidate out of a strong aversion towards smokers.[43] Two scenarios can be envisaged:[44]

(a) Discrimination by a human agent. The illicit motive remains hidden *in interiore hominis*, and the recruiter may even claim that smoking is not expressly a protected ground.[45]

(b) Discrimination by an AI system. By contrast, stochastic LLMs or probabilistic deep learning models[46] acquire and refine their behaviour through "experience"[47] in real or simulated environments, building models upon an

---

[39] As discussed earlier according to this approach, the assessment of a discriminatory phenomenon must instead concentrate on its concrete effects, considering, as already discussed, not only the variability of indices and classes but also the very absence of intentionality.

[40] Kleinberg (n 7) 28; C R Lawrence III, 'The Id, the Ego, and Equal Protection: Reckoning With Unconscious Racism', (1987) 39 Stan Law Rew. 317.

[41] Kleinberg (n 7) 37.

[42] In this sense, according to the behaviourist perspective previously outlined, a factual equivalence is drawn between the conduct of the human agent and that of the machine agent. By contrast, to believe that the use of the latter could put an end to millennia-old problems, such as the very definition of discrimination, is a technophilic and fallacious misconception and, as in the case of liability, more often than not a fraudulent one: E Morozov , *To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exists* (Public Affairs, 2013).

[43] A similar example has been advanced in the literature regarding a recruiter who discriminates against a candidate based on the applicant's zodiac sign: P S Shin, 'Is there an unitary concept', (n 4), 17-18.

[44] This analysis does not engage with those doctrines which maintain that no discriminatory treatment arises where the criterion invoked by the subject is one of their own characteristics and is attributable to their own fault. On this point, see E Pariotti, **'** "Vulnerabilità e diritto" '(2019) 2 Ars Interpr. 13.

[45] If one assumes the necessary correlation between a illicit motive or action and a legal index Consiglio (n 4) 84.

[46] Z Ghahramani, 'Probabilistic machine learning and artificial intelligence' (2015) 521(7553) Nature 452.

[47] Here the noun *experience* is employed in an improper sense. Machines are in fact regarded as lacking phenomenal consciousness. On this distinction, see N Block, 'On a Confusion about a Function of

enormous number of parameters that render the resulting decisions potentially irreproducible and unpredictable.[48] Such phenomena can be linked to reinforcement learning techniques,[49] which enable the system to update its inferences based on new information, thereby emphasising correlations that were not anticipated at the design stage. Within this framework, a system even when trained to comply with anti-discrimination norms, for instance by excluding legally protected sensitive features may nonetheless deviate from them in practice.[50] In a manner analogous to the human case, such a system might identify a statistical correlation between reduced work efficiency and smoking, inferred from yet another correlation between smoking and the worker's geographical location.[51] However, unlike the human agent, a sort of zero-sum game emerges: while the human will almost certainly dissemble the illicit intent, the machine may instead expose its bias and expressly exclude the smoker.

In this latter example, the more formalistic interpreter must evaluate the empirical and factual singularity within which it occurs, moving beyond the rigid reliance on indices and classes in evaluation as well as the supposed necessity of intention.

From this perspective, LLMs may become a cultural *leitmotiv* that destabilises the positivist methodology; a sort of "moral mentors": [52] not because machines surpass human ethics, but because they expose the fractures of a positivised system that merely reproduces market interests in legally relevant decisions. [53]

Beyond this expectation or rhetorical suggestion, the underlying problem, however, remains primarily cultural rather than technological. [54] Liberal rhetoric has long confined strict liability to exceptional cases, labelling it anachronistic,[55] when the presence of causation and intent is required.[56] As also

---

Consciousness' (1995) 18 Behavioral and Brain Sciences 227, where the author, in criticising computational theories of consciousness, distinguishes between phenomenal consciousness and access consciousness: the former consists of specific experiential mental states, that is, the qualitative properties of experience that render a situation consciously "lived." Nonetheless, at least from the perspective of civil law, theorising machine consciousness reflects merely an anthropomorphic anxiety, without altering the framework of responsibility. On this point, see Battaglino (n 7) 663-666.

[48] W Xin Zhao and others, 'A Survey of Large Language Models' [2023] arXiv:2303.18223, 1.

[49] T Lesort and others, 'Understanding Continual Learning Settings with Data Distribution Drift Analysis' [2022] arXiv:2104.01678, 1.

[50] D Tafani, 'Sulla moralità artificiale. Le decisioni delle macchine tra etica e diritto' (2020) 1 Riv. Fil 81.

[51] G Gometz, 'Intelligenza artificiale' (n 27) 27-28.

[52] The idea of the machine as a moral mentor has now ignited a debate in philosophy, is no longer confined merely to the realm of literature (for those who distinguish between the two). One may think, for example, of *Solaris* by Stanisław Lem, or of the relationship between Wagner and the homunculus in Goethe's *Faust*, to cite a more erudite reference. For relevant bibliography on this topic, see F Fossa, 'Artificial moral agents: moral mentors or sensible tools?' (2018) 20(1) Ethics Inf. Technol. 1 ff.

[53] But there is more. Certain discriminatory phenomena protected under anti-discrimination law, such as harassment or exploitation, require a bio-mechanical component which, at present, machines do not appear to possess. This problem may therefore be relegated either to technophobia or to the realm of science fiction.

[54] P Femia, 'Minus ut valeat: l'impossibilità di una regolazione giuridica metaculturale', in VV.AA *I rapporti civilistici nell'interpretazione della Corte costituzionale nel decennio 2006-2016* (ESI, 2020) 357 ff.

[55] On the individualistic and anachronistic conception that confines the application of strict liability to an exception, compare Battaglino (n 6) 636.

[56] Nardocci (n 4) 2372.

becomes evident in the evaluation of indices, this approach does not primarily presuppose substantive protection.[57]

This formal logic equally extends to the sphere of contractual liability, where an expansion of liability would raise no problem of causation or intention.[58] Here too, this rhetoric operates through subsumption, employing the historical liberal techniques of binarization and confinement:[59] whatever is not expressly included in the contract is deemed legally irrelevant, while what is included becomes valid by default: *qui dit contractuel dit juste*.[60] In this way, contractual liability is often reduced to a residual category vis-à-vis tort liability[61]; and, where the latter is invoked, liberal theory tends to cling to the moralisation of the agent, insisting on the necessity of fault, of a material causal nexus, and on the exceptional character of strict liability. Modern theory, however, has long since overcome the identification of the obligatory relationship with the mere duty of performance, recognising instead the relevance of additional and ancillary obligations. In this perspective, the "contractual" qualification of liability operates as a synecdoche: what is truly at stake is a conceptual shift from the paradigm of breach of the contract-as-act to that of breach of the obligation tout court.[62]

---

[57] Insisting on subsumption into indices in the name of mere legal certainty and predictability On the relationship between subsumption, positivism, legal certainty and liberal culture, reference may be made to the bibliography in Battaglino (n 6) 616-628.

[58] On this point, see C Castronovo, 'Swinging malpractice Il pendolo della responsabilità medica' (2020) 3 883 ff.

[59] In this sense see Femia (n 4) According to this view, *binarisation* is the condition by which multilaterally complex social interaction is reduced to the iteration of two contracting parties; *confinement*, in turn, represents its functional corollary, whereby social relations are confined within what is deemed to be valid or invalid solely on the basis of what is contractually stipulated. Within this framework, anything that does not conform to contractual relativity, to the logic of party/third party, or more generally to a network of simple, confined, and binary units, remains excluded from the contractual sphere and thereby relegated to regulatory indifference within the cognitive operations of the contractual system. In this respect, within common law jurisdictions, the attribution of contractual liability to an act of will, or, more strongly, to the presence of consideration, beyond which lies only tort, amounts to a form of binarisation.

[60] It has by now become a mere capitalist slogan, despite the meaning originally intended by Alfred Jules Emile Fourié.

[61] *Contra* C Castronovo, 'La relazione come categoria essenziale dell'obbligazione e della responsabilità contrattuale' (2011) 1 Eur. Dir. priv., *passim.*

[62] Liberal theses which exclude contractual liability when discrimination occurs "outside the contract" are grounded in a formal and static conception of contractual responsibility. Within such an ordinary configuration, certain cases would be excluded from liability for the absence of a contract as a formal act and, even more so, for the lack of a consideration, its constitutive nucleus, as provided since the Romanist tradition. Modern theory, however, precisely through a substantive approach, has long since moved beyond the identification of the obligatory relationship with the sole obligation of performance, recognising instead the significance of duties other than prestation. From this perspective, the "contractual" characterisation of liability functions as a synecdoche, as what is at stake is a conceptual shift: from the violation of the contract-as-act to the violation of obligation *tout court*. It follows that contractual liability may arise even in the absence of a formal act, provided that an obligation, whose source may differ from the contract itself, has been violated. On this point, see for Example: V Cuffaro, *Responsabilità precontrattuale,* in *Enciclopedia del Diritto*, XXXIX, Milano, 1988, 1270 e C Castronovo, *La responsabilità civile,* cit., 524. C Castronovo, *Sul significato di materia contrattuale,* cit., 518-519 Similarly, even in markedly liberal systems, though some fifty years later than German doctrine, the traditional individualistic conception of contract has been surpassed in favour of a vision of social solidarity, whereby contractual liability may be invoked even beyond the traditional barriers of privity and consideration: EH Hondius, *Precontractual Liability: Reports to the XIIIth Congress, International Academy of Comparative Law, Canada, 18–24 August 1990* 5 ff. It follows that contractual liability may also arise in the absence of a formal act, provided that an obligatory bond has been breached, the source of which does not necessarily coincide with the contract itself. See, inter alia, C Castronovo, *La nuova responsabilità civile*, cited above, *passim.* Similarly, even in markedly liberal legal systems – albeit with a delay of approximately fifty years compared to German doctrine – the traditional

It follows that the problem does not lie in the absence of a new legislative prohibition, such as a statute expressly banning discrimination by machines or regulating their use as such; rather, it remains cultural and hermeneutic. A substantive and functional approach to interpretation is capable of setting meaningful limits to discriminatory phenomena, regardless of whether the agent is human or artificial.

Rather, it is the interpreter, and not politics or formal law alone,[63] who must take up the task of confronting the injustice of discriminatory phenomena.

In conclusion, as suggested by Kleinberg, the machine may play a constructive role: whether in extra-contractual or contractual liability, it may function as a heuristic trigger that prompts a retrospective and genuinely multifactorial assessment of discrimination across all stages of the facts.[64] In this way, processes, rule-systems, practices, or institutional arrangements , even when apparently neutral and impersonal, such as anti-discrimination law itself, may, once considered in their concrete effectiveness, reveal a treatment whose absolute constant may be identified in the violation of human dignity.[65] And if civil law is to commit itself, by every available means, to combating an injustice, then its remedies must not appear anachronistic in relation to a phenomenon whose complexity grows in step with economic and technological development.[66]

individualistic conception of contract has been superseded in favour of a vision grounded in social solidarity, by virtue of which contractual liability may also be invoked beyond the traditional barriers of privity and consideration. In this regard, EH Hondius, *Precontractual Liability: Reports to the XIIIth Congress, International Academy of Comparative Law*, Canada, 18–24 August 1990, 5 ff. For further discussion, see the relevant bibliography in G Battaglino, L Pandolfelli, 'Per una responsabilità contrattuale dei marketplace' (2025) 3 Riv. crit. dir. priv. 369-385.

[63] On this point, see Nardocci (n 4) 2369-2372.

[64] In legal scholarship, there is also debate as to the temporal moment at which the prohibition of discrimination should operate within contractual dealings. Some argue for its application only after negotiations have taken place and, therefore, once the contract has been concluded. Yet, once again, those who deny that contractual liability may apply at every stage of the contractual process reproduce the liberal vision of binarisation and confinement. On this point, see the bibliography cited in note 4.

[65] Gentili (n 4) 216.

[66] The market, in fact, as an artificial construct, does not appear to reduce the phenomenon of discrimination in any meaningful way., SJ Schwab, 'Un approccio di law and economics alla teoria della Discriminazione nei rapporti di Lavoro', in P Inchino (ed), *Lezioni di diritto del lavoro. Un approccio di labour law and economics* (Giuffrè 2004) 347 ff.

D'Aloia DS, 'Il token immobiliare nel contesto del codice civile italiano' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252DSDA

EJPLT
ISSN 2704-8012



Il token immobiliare nel contesto del codice civile italiano

The real estate token in the context of the Italian civil code

DAVIDE SILVIO D'ALOIA
Ph.D., Avvocato
Università degli Studi Suor Orsola Benincasa

Abstract

L'alienabilità del token immobiliare crea nuove sfide per il diritto civile, poiché implica la trasposizione digitale di situazioni giuridiche reali su blockchain. Il presente studio analizza la validità e opponibilità delle operazioni dispositive aventi a oggetto token rappresentativi di diritti reali immobiliari, interrogandosi sulla necessità di un regime di pubblicità che assicuri certezza ai terzi. Adottando un approccio Law & Economics, si valutano funzionalità ed elasticità del sistema civilistico italiano, anche alla luce dei costi e benefici delle soluzioni decentralizzate. Viene esaminata la possibilità di coordinare la pubblicità immobiliare tradizionale con i registri distribuiti e la compatibilità della compravendita di token immobiliari con gli istituti della vendita a misura, della multiproprietà e della multiproprietà azionaria. L'obiettivo è verificare se e in che misura la blockchain possa integrare o sostituire la trascrizione nei registri immobiliari.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
The alienability of the real estate token creates new challenges for civil law, as it implies the digital transposition of real legal situations on blockchain. This study analyses the validity and enforceability of dispositive transactions involving tokens representing real property rights, questioning the need for a publicity regime that ensures certainty for third parties. Adopting a Law & Economics approach, the functionality and elasticity of the Italian civil law system is assessed, also in light of the costs and benefits of decentralised solutions. The possibility of coordinating traditional real estate advertising with distributed registers is examined, as well as the compatibility of the purchase and sale of real estate tokens with the institutes of the sale by measure, timeshare and time-share. The aim is to verify whether and to what extent blockchain can complement or replace transcription in real estate registers.

Keywords: token immobiliare; Real Estate; codice civile; trascrizione; digital asset; metodo Law&Economics

Summary: 1. Introduzione. – 2. La tokenizzazione nel settore Real estate: definizione ed impatto sul mercato. – 3. Il token immobiliare: una classificazione possibile ed i profili di criticità. – 4. Il vulnus del regime di trascrizione e i modelli europei di circolazione dei token. – 5. L'art. 2645 c.c. secondo il metodo *Law&Economics*. – 6. Possibili istituti affini alla compravendita di un token immobiliare. – 7. Una conclusione che sa di introduzione.

1. Introduzione.

L'alienabilità di un token immobiliare, nel senso di token rappresentativo di un diritto di proprietà o altro diritto reale su un bene immobile fisico, solleva questioni complesse sotto il profilo civilistico, in quanto implica la trasposizione, in ambiente digitale, di situazioni giuridiche reali, aventi ad oggetto beni immobili.

Il token, quale rappresentazione digitale su tecnologia blockchain di un diritto reale immobiliare (ovvero di una sua frazione o di una posizione contrattuale ad esso riferita), pone interrogativi sia in ordine alla validità e opponibilità delle operazioni dispositive, sia in relazione alla necessità di un regime di pubblicità che ne assicuri la certezza nei confronti dei terzi.

In particolare, l'eventuale riconducibilità dell'alienazione di un token immobiliare alla fattispecie prevista dall'art. 2643 c.c. e ss. solleva il problema dell'assoggettabilità di tale trasferimento alla trascrizione nei registri immobiliari, nonché della compatibilità tra quest'ultima e la registrazione su blockchain.

Il percorso di analisi seguirà, quindi, due direttrici principali: da un lato, l'analisi della natura giuridica del token rappresentativo di un bene immobile, il cd. token immobiliare; dall'altro, una valutazione in ordine alla possibilità di coordinare il sistema tradizionale della pubblicità immobiliare con i registri digitali distribuiti, valutando se e a quali condizioni la trascrizione possa essere sostituita, integrata o surrogata da strumenti tecnologici alternativi.

In tale contesto, il presente lavoro adotta un approccio metodologico ispirato al modello interpretativo *Law&Economics*, al fine di individuare soluzioni che non si limitino a una ricostruzione sistematica in chiave dogmatica, ma che tengano conto del diritto in chiave agnostica, valutando se le altre scienze, in primis l'economia, possano spiegare il diritto e renderlo adattivo ad una società dinamica[1].

In quest'ottica, il diritto viene visto come uno strumento che deve parametrarsi a standard pratici e non ermeneutici, e l'interprete deve cercare ogni scienza sociale, al di fuori del diritto, per incidere sul diritto stesso[2].

Per dovere di chiarezza, il metodo del *Law&Economics* si differenza dal metodo della analisi economica del diritto, definito troppo "aggressivo e riformista"[3], in quanto - valutando l'efficienza allocativa delle regole giuridiche, del contenimento dei costi di transazione e della certezza dei traffici giuridici - utilizza l'economia per analizzare il mondo del diritto, come una leva archimedea che permette allo studioso di argomentare in favore del cambiamento di un sistema giuridico.

Le soluzioni dell'analisi economica del diritto sono due: da un lato, verificare se un impianto normativo offra strumenti capaci di essere spiegati in chiave economica; dall'altro, anche al netto di possibili modifiche normative, se il sistema giuridico non risulti adatto, in chiave economica, ne viene dichiarata l'irrazionalità.

L'approccio *Law & Economics*, quale metodo interpretativo sociale del diritto, dunque - assumendo come punto di partenza l'art. 2645 c.c. - consente di analizzare l'effettiva funzionalità ed elasticità del sistema civilistico italiano e dell'istituto della trascrizione in riferimento alla categoria dei token immobiliari, non solo quale meccanismo formale di pubblicità, ma anche come strumento di minimizzazione del rischio di conflitti tra acquirenti e di riduzione dell'asimmetria informativa.

L'interazione tra tecnologia blockchain e sistema dei registri pubblici viene esaminata anche alla luce dei costi e benefici associati a ciascun modello, con l'intento di verificare se e in che misura le soluzioni decentralizzate possano assicurare livelli di certezza e affidabilità equivalenti o superiori a quelli offerti dal sistema tradizionale della trascrizione e, più in generale, del sistema civilistico italiano.

---

[1] G. CALABRESI, A. D. MELAMED, *Property Rules, Liability Rules and Alienability: One View of Cathedral*, in *Harv. L. Rev.*, 1972, 85, 1089, in cui gli A. ricorrono alla metafora della Cattedrale di Rouen osservata da Monet nelle diverse visuali determinate dai toni di luce che si susseguono nel corso del giorno, per spiegare la natura "poliedrica" del diritto, incline alla contaminazione con scienze esterne dal diritto e capaci di incidere sul diritto stesso.

[2] Questo è quanto il professor Calabresi ha teorizzato con l'espressione "Law&...", al fine di riformare il mondo del diritto. Sul punto G. CALABRESI, *An introduction to legal thought: four approaches to law and to the allocation of body parts*, in *SLR*, 2003, 55, 2113-2152. Si veda anche E.J. WEINRIB, *The idea of private law*, 2ª ed., Oxford, 2012, 12-13. Vien da sé chiedersi, dunque, alla luce del contesto sopra descritto, se sia immaginabile un metodo interpretativo del tipo "Law&Technologies", per il quale le tecnologie assurgerebbero ad essere uno strumento interpretativo della norma e non solo l'oggetto della norma, permettendo così di adattare il diritto vigente al progresso del contesto sociale e non di stravolgerlo in funzione del progresso. Il rapporto tra diritto e tecnologia, dunque, deve essere visto in un'ottica futura, pur conservando la forza delle categorie giuridiche vigenti.

[3] Sul punto si tengano in debita considerazione AA. VV., *Il futuro del Law and Economics. Saggi per una rimeditazione ed un ricordo*, a cura di F. FIMMANÒ e V. OCCORSIO, Milano, 2018, 8.

2. La tokenizzazione nel settore Real estate: definizione ed impatto sul mercato.

La tokenizzazione nel settore immobiliare è un'espressione che indica la nuova frontiera di utilizzo o acquisto di un immobile fisico.

Il processo di digitalizzazione dell'asset reale permette, infatti, una nuova forma di relazione con l'investimento che si può realizzare anche attraverso la creazione di particolari token che circolano su piattaforme blockchain, come verrà spiegato più approfonditamente a breve[4].

Il fenomeno è stato per la prima volta, nel 2014, definito come *Proptech*, dall'unione delle parole *property* e *technology*.

La *Proptech*, pertanto, si qualifica come un nuovo modo di interpretare il *Real estate*, che si è definitivamente aperto al mondo della tecnologia, con riferimento all'incontro tra i soggetti che intervengono nelle compravendite e nei negozi giuridici che attengono ai beni immobili, evidenziando l'incontro a livello negoziale tra costruttori, intermediari, consumatori, ovvero tra tutti i soggetti interessati allo scambio immobiliare.

Le startup che sfruttano questi strumenti, sostituendo il lavoro dei professionisti con la tecnologia, eseguono le stesse fasi della compravendita immobiliare rispetto alle agenzie tradizionali, differenziandosi da quest'ultime, già dalla fase di valutazione dell'immobile.

La *Proptech*, infatti, impiega specifici algoritmi online per quantificare in modo completamente oggettivo il valore di mercato, incrociando i dati su domanda, offerta e area di interesse.

Tutto ciò avviene confrontando il valore di mercato stimato di un immobile con il valore di altri immobili simili, per caratteristiche e ubicazione.

È perciò evidente che il criterio di valutazione adottato dalla *Proptech* rappresenti un notevole progresso nel settore immobiliare, in quanto elimina qualsiasi componente soggettiva nella stima del valore che un professionista potrebbe effettuare, basandosi su algoritmi matematici con un margine di errore minimo e trascurabile.

Inoltre, anche nella fase di visita dell'immobile, la *Proptech* utilizza la tecnologia sfruttando i *virtual tour*, eliminando così l'incontro fisico tra il potenziale acquirente e il professionista, riducendo i tempi e modificando in maniera significativa le modalità operative degli agenti immobiliari[5].

---

[4] Sull'importanza del processo di tokenizzazione dei beni, non solo nel contesto off-chain ma anche nel contesto del metaverso, si tenga in debito conto R. BOCCHINI, *Nuovi beni digitali e mondi dematerializzati. Il metaverso*, in *EJPLT*, 2023, 1, 50, in cui l'A. precisa: «[…] Tutte le piattaforme, che sono ovviamente gestite dalle principali società di tecnologia al mondo, come per esempio Decentraland, Meta, Nvdia, Unity, Apple, Microsoft, Google, Amazon, creano, con un'evoluzione dei social media e facendo sempre più entrare gli utenti in un mondo sintetico che deve coniugare la vita reale con quella virtuale permettendo di acquistare beni immobili e ben mobili. Le aziende si stanno attrezzando per tokenizzare il nuovo ecosistema digitale ed entrare in tutti i settori del commercio dall'arte digitale ai viaggi, all'istruzione, al real estate ed è, quindi, necessario analizzare ad oggi come è possibile far fruire gli utenti di questi nuovi beni. […]».

[5] Talune agenzie immobiliari online, annoverabili tra le proptech, hanno il vantaggio di appoggiarsi ad applicazioni che permettono al potenziale venditore di creare il proprio annuncio, fornendo modelli preimpostati da compilare online, nonché di prenotare, gestire e consultare gli appuntamenti di visita virtuale dell'immobile da parte di possibili acquirenti. Infatti è opportuno evidenziare, come di seguito si spiegherà, che le proptech non sono una minaccia per il settore immobiliare tradizionale, quanto piuttosto un punto di partenza verso un suo sviluppo. Il settore immobiliare su piattaforme come eToro ha subito cambiamenti significativi, soprattutto grazie all'integrazione di nuove tecnologie e all'evoluzione delle

Un esempio di piattaforma *Proptech*, completamente made in Italy, è *Rexer*, una agenzia immobiliare di nuova generazione capace di sviluppare e valorizzare le attività nel *Real estate*[6].

Quel che preme qui sottolineare è che si tratta di una agenzia/piattaforma digitale che utilizza sia la tecnologia dei *Big data* per fornire una stima del valore di ogni immobile rispetto agli immobili simili nella stessa area geografica, sia l'intelligenza artificiale generativa per la fase di elaborazione degli annunci.

Questo tipo di piattaforma *Proptech*, come altre già esistenti nel panorama europeo e oltreoceano, rappresentano quella che si può definire come fase di "digitalizzazione del mercato immobiliare", dove l'utilizzo dell'AI, *lato sensu*, si limita ad essere un sostegno alla compravendita immobiliare che, allo stato, resta ancorata a norme abbastanza stringenti, che non permettono l'utilizzo delle tecnologie per tutte le fasi del *Real Estate*.

Tuttavia quello che si vuole far emergere in questo contributo, è la presenza di piattaforme blockchain sulle quali è possibile direttamente acquistare beni immobili o porzioni di esso (token immobiliari), aprendo le porte ad una possibile *Proptech 2.0*, dove la digitalizzazione non si ferma alla sola visita guidata di un immobile, o alla raccolta e gestione delle informazioni e dei documenti necessari per la compravendita, tramite soluzioni digitali evolute, ma consente direttamente l'acquisto della proprietà o di una quota di comproprietà dell'immobile fisico.

---

strategie di investimento nel 2024. Tra le principali tendenze si annoverano: 1.Influenza tecnologica: L'intelligenza artificiale (AI) sta diventando uno strumento fondamentale per gli investitori immobiliari. AI viene utilizzata per analizzare grandi quantità di dati, valutare i prezzi delle proprietà e persino prevedere le tendenze future. Questo non solo rende il processo di investimento più efficiente, ma fornisce anche una visione predittiva più accurata, permettendo agli investitori di identificare opportunità che potrebbero non essere evidenti con i metodi tradizionali. 2. Cambiamento nel settore immobiliare commerciale: Con l'aumento del lavoro a distanza, gli uffici commerciali stanno registrando tassi di vacanza più elevati. Di conseguenza, gli investitori stanno spostando l'attenzione verso proprietà retail e multifamiliari, considerate più resilienti. Questi spazi retail adottano concetti innovativi che combinano lavoro, svago e abitazione per rispondere ai nuovi comportamenti dei consumatori. 3. Dinamiche di mercato: Nonostante l'aumento dei tassi di interesse e la diminuzione dei volumi di transazioni, gli investitori immobiliari mostrano un cauto ottimismo. I prezzi delle case restano alti a causa della forte domanda, ma ci sono segnali che indicano un raffreddamento del mercato, il che potrebbe creare nuove opportunità per gli acquirenti alla prima esperienza, con un aumento delle proprietà disponibili sul mercato. 4. Tendenze globali: Al di fuori degli Stati Uniti, mercati come l'India stanno registrando una forte domanda per alloggi di lusso, grazie all'urbanizzazione e a politiche governative favorevoli. Dal punto di vista statistico, nel 2024, circa il 12% degli investitori su eToro ha destinato una parte del proprio portafoglio agli investimenti immobiliari. Questo dato, pur inferiore rispetto a settori come la tecnologia, mostra un interesse crescente verso beni immobili più tradizionali, soprattutto a causa dell'aumento dei tassi di interesse e dell'inflazione. Ulteriori informazioni sono disponibili al seguente link: https://www.etoro.com/smartportfolios/realestatetrusts

[6] Si tratta della prima forma di piattaforma italiana digitale aperta agli operatori del mercato immobiliare, nata nel primo trimestre del 2024 dalla partnership tra Intesa Sanpaolo, la proptech del Real Estate Homepal e gruppo Bper Banca. Con questa operazione, Intesa Sanpaolo parteciperà, con il 100% di Intesa Sanpaolo Casa, al capitale di Homepal con una quota del 49%; il restante capitale sarà detenuto per il 34% dalla attuale compagine societaria di Homepal e per il 17% da Bper Banca. La mission di Rexer è: offrire un servizio che permetta ai clienti di essere seguiti e, allo stesso tempo, di conservare il pieno controllo delle attività: mettendo le esigenze del cliente al centro di ogni azione, supportandolo con professionisti esperti e con la tecnologia, dalla pubblicazione dell'annuncio alla conclusione dell'affare; facilitando il rapporto tra agenzia e cliente, trasformando una fredda relazione di business in un dialogo aperto e caldo; offrendo un servizio di valore, che accompagni per mano il cliente. Promuovere la collaborazione con partner industriali e banche che vogliano partecipare allo sviluppo di un nuovo modello di crescita, attraverso il concetto di Open Proptech Platform. Per maggiori informazioni visitare il link: https://rexer.it/chisiamo

Un esempio di piattaforma blockchain nel settore immobiliare, è la start-up italiana *RElabs*[7], la quale è in grado di sviluppare una vasta gamma di soluzioni ad alto contenuto tecnologico, tra cui: lo *smart building*, la "patente digitale" di un immobile con tutte le informazioni relative alla proprietà e alle pratiche catastali e la tokenizzazione degli immobili.

Un esempio concreto di applicazione della blockchain al settore immobiliare, offerto da *RElabs* è l'appalto per la manutenzione di un immobile.

L'impiego della tecnologia blockchain consente di attribuire all'appaltatore, incaricato della manutenzione di una pluralità di immobili, l'onere di inserire un input nel sistema informatico messo a disposizione da *RElabs*. Tale dato, una volta registrato nel «registro digitale condiviso» basato su tecnologia blockchain, acquisisce carattere di immutabilità, risultando non più modificabile.

In tale contesto, la società committente non è più tenuta a inviare propri incaricati per verificare in loco l'avvenuta esecuzione delle singole prestazioni, potendo invece fare affidamento sulla prova informatica dell'intervento effettuato in un dato momento da uno specifico operatore dell'impresa appaltatrice. Qualora emerga che l'appaltatore abbia inserito dati mendaci, la controparte dispone di una prova certa della condotta imputabile e potrà attivare le clausole sanzionatorie previste per l'inadempimento.

Si tratta di un esempio emblematico del potenziale innovativo della blockchain nei rapporti contrattuali: riduzione degli oneri di controllo, semplificazione procedurale, maggiore trasparenza e rafforzamento della tracciabilità delle responsabilità.

L'esempio di *RElabs*, in ambito di tokenizzazione immobiliare, è un chiaro segno di come essa, unitamente alla circolazione in blockchain dei token stiano aprendo le porte ad un numero sempre più elevato di investimenti.

È interessante, dunque, approfondire i diversi vantaggi della tokenizzazione immobiliare, partendo dall'assunto che con essa si realizza una riduzione dei costi transattivi, grazie alla disintermediazione, con un marcato impatto nel caso di transazioni con elementi di natura transnazionale[8].

La riduzione dei costi transattivi, inoltre, può rendere economicamente praticabili investimenti, anche in quote molto piccole, di beni che generalmente fungono da riserva di valore, favorendo la liquidità del mercato, democratizzandolo, grazie all'offerta di nuove opportunità di investimento fruibili da un'ampia platea di sottoscrittori.

La tokenizzazione di un immobile favorisce una vasta platea di investitori potenziali, prestatori di denaro, limitando il numero di quote/token alla sola quantità utile a soddisfare l'esigenza del proprietario bisognoso di un prestito, con la possibilità di tokenizzare, in presenza di future esigenze, altre porzioni, senza che i nuovi investitori/prestatori possano avere limiti derivanti dalla presenza di ipoteche di grado precedente.

---

[7] RElabs, la prima società in Italia specializzata nell'utilizzo della tecnologia blockchain nel Real Estate, nasce dalla

Per maggiori informazioni in ordine alla attività in blockchain di RElabs, visitare il sito: https://www.relabs.it/#servizi

[8] Sul punto si tenga conto di R.M. GARICA TERUEL, *Legal challenges and opportunities of blockchain technology in the real estate sector*, in J. *Prop. Planning and Envir. L.*, 2020, 12, 2, 129 ss.

Dunque, visti questi aspetti positivi, anche a livello concreto la tokenizzazione immobiliare ha registrato una crescita significativa, specialmente su scala globale, sfruttando la tecnologia blockchain per trasformare diritti di proprietà su beni immobili in token digitali.

Secondo una stima di *Security Token Market*, il valore degli asset tokenizzati potrebbe raggiungere i 30 trilioni di dollari entro il 2030, in riferimento ad attività immobiliare[9].

Oltreoceano la tokenizzazione immobiliare sta guadagnando terreno, con diverse piattaforme che offrono opportunità di investimento frazionato in proprietà reali[10]. Un esempio lampante è il *St. Regis Aspen Resort*, un lussuoso hotel situato ad Aspen, il quale è stato tokenizzato per consentire investimenti frazionati, permettendo agli investitori di acquistare quote dell'hotel tramite blockchain e beneficiare dei ritorni economici generati dalla proprietà[11].

In Europa, la tokenizzazione degli asset finanziari sta guadagnando slancio, con una crescita del 43% nel 2024, secondo l'*Osservatorio Blockchain* e *Web3* del Politecnico di Milano.

Tuttavia, la tokenizzazione specifica del settore immobiliare procede a un ritmo più lento, principalmente a causa di incertezze normative e della frammentazione del mercato europeo.

Nonostante la difficoltà del contesto europeo, comunque, secondo un'analisi di *PwC Italia*[12], si prevede che la tokenizzazione degli asset illiquidi raggiungerà i 16.000 miliardi di dollari entro il 2030, evidenziando il potenziale significativo di questo mercato.

Tuttavia, l'adozione varia tra i paesi europei, con alcune nazioni che avanzano più rapidamente grazie a regolamentazioni più favorevoli.

In Italia, il mercato della tokenizzazione è ancora agli inizi.

Secondo l'*Osservatorio Blockchain & Web3*[13] del Politecnico di Milano, gli investimenti in blockchain nel paese sono stati di circa 40 milioni di euro nel

---

[9] Fonte CoinDesk: https://www.coindesk.com/it/opinion/2025/02/07/rwa-tokenization-is-going-to-trillions-much-faster-than-you-think?utm_source=chatgpt.com

[10] Si veda ad esempio la piattaforma RealT, piattaforma statunitense con sede in Florida, la quale consente agli investitori di tutto il mondo di acquistare nel mercato immobiliare statunitense tramite una proprietà tokenizzata, frazionata e pienamente conforme, il tutto grazie alla blockchain. Maggiori informazioni sono disponibili al seguente link: https://realt.co/

[11] F. VENTURA, *Token immobiliari: il futuro del mercato immobiliare?*, in *V-Tech Studio*, 14 gennaio 2025, disponibile al link: https://www.francescoventura.it/token-immobiliare/#utm_source=chatgpt.com

[12] Per maggiori informazioni, consultare il link: https://www.pwc.com/it/it/publications/docs/Tokenizzazione.pdf

[13] L'Osservatorio nasce nel 2018 con il nome di Osservatorio Blockchain & Distributed Ledger e nel 2023, per rispondere all'evoluzione delle applicazioni di queste tecnologie, cambia il nome in Osservatorio Blockchain & Web3. La mission dell'Osservatorio è generare e condividere la conoscenza sui temi Blockchain e Web3 e contribuire allo sviluppo del mercato italiano e internazionale, creando occasioni di incontro e confronto tra i principali attori attivi sul tema. Dal 2021 inoltre l'Osservatorio ha attivato anche il Blockchain Innovation & Solutions HUB, un laboratorio super partes che si pone l'obiettivo di promuovere, facilitare e abilitare progetti in ambito Blockchain coinvolgendo attori differenti, attraverso la creazione di un ambiente di sviluppo precompetitivo dove le aziende possano svolgere attività di ricerca applicata. L'Osservatorio Blockchain & Web3, all'interno dell'edizione annuale, si propone di svolgere le seguenti attività di Ricerca: 1. cinque filoni di ricerca business: mercato internazionale: analisi dei progetti internazionali e dell'utilizzo delle tecnologie Blockchain da parte di aziende startup a livello globale; mercato italiano: analisi dei progetti e delle startup attive in Italia e indagine sull'adozione di crypto-asset da parte dei consumatori italiani; Internet of Value: analisi dello stato di evoluzione e di adozione di cripto-valute, stablecoin e Central Bank Digital Currency (CBDC); Blockchain for business: analisi dell'impatto delle tecnologie Blockchain e della tokenizzazione sugli ecosistemi di business esistenti e sui processi delle aziende; Decentralized web: analisi delle principali applicazioni decentralizzate (DApp) e dei settori di applicazioni più rilevanti del web3:

2024, con una crescita del 5% rispetto all'anno precedente. Questa cifra rimane modesta rispetto ad altri paesi europei, indicando una necessità di maggiore sviluppo e adozione di una normativa adatta nel settore[14].

Attraverso il processo di tokenizzazione, dunque, si rende possibile dividere in più token un unico immobile, così da consentire a più soggetti che lo acquistano, di esercitarvi diritti (i cd. *metadata*).

Tuttavia, nonostante gli indubbi vantaggi portati dalla tokenizzazione immobiliare, permangono degli annosi problemi in riferimento al sistema civilistico italiano, tali da rendere difficoltosa la concreta operabilità della *Proptech 2.0*; e più precisamente permane il problema di riuscire a qualificare il token immobiliare quale titolo di proprietà su un bene immobile fisico (problema della natura del token) ed il problema del rapporto tra la circolazione in blockchain dei token ed il regime di trascrizione previsto dal codice civile italiano.

3. Il token immobiliare: una classificazione possibile e i profili di criticità.

In ordine al problema della natura del token immobiliare, in un'ottica di relazione tra la tokenizzazione del *Real estate* ed il sistema civilistico italiano, ed una conseguente lettura interpretativa di quest'ultimo alla luce del metodo *Law&Economics*, sorgono alcuni profili di criticità.

Si pensi al caso in cui un individuo Alpha proprietario del bene immobile Gamma, per esigenze legate ad una maggiore liquidità, decida di convertire la tradizionale proprietà del suo immobile, in una *smart property*: in altre parole, il titolo di proprietà sul bene Gamma viene frazionato in piccole unità (token), le quali vengono trasferite - a mezzo di smart contracts su piattaforme di blockchain - al Sig. Beta, Sig. Caio e Sig. Tizio.

Seppur dal punto di vista economico questa operazione presenta indubbi vantaggi, tuttavia è sul piano giuridico che sorgono delle perplessità.

Sulla natura di ogni singolo token immobiliare, l'attuale opinione dottrinale è divisa tra chi ritiene che il token immobiliare sia un NFT e chi ritiene che il token immobiliare rientri nella categoria dei *financial token*.

Decentralized Finance (DeFi), Non Fungible Token (NFT), Decentralized Autonomous Organizations (DAO), Self-Sovereign Identity (SSI), Metaverso decentralizzato. 2. sei filoni di ricerca tech: DAO e governance token: analisi delle modalità di creazione e funzionamento delle Decentralized Autonomous Organizations; Data privacy: identificazione delle modalità con cui è possibile controllare la visibilità delle informazioni nelle piattaforme Blockchain; performance, scalabilità e consumo energetico: identificazione delle differenze e delle possibilità per colmare il gap tra le attuali performance delle piattaforme Blockchain esistenti e quelle richieste nelle varie applicazioni; interoperabilità: analisi dei principali approcci all'interoperabilità tra piattaforme Blockchain differenti e dei potenziali benefici; confronto tra piattaforme: monitoraggio continuo delle piattaforme principali e più interessanti; confronto delle loro caratteristiche attraverso un'analisi delle variabili maggiormente rilevanti; convergenza con altre tecnologie: monitoraggio dell'interazione delle tecnologie Blockchain con altre tecnologie (es. AI, IoT). 3.un filone di ricerca legal: regolamentazione e normativa: mappatura delle principali regolamentazioni di impatto sul mondo Blockchain e analisi delle modifiche normative più rilevanti in relazione alle applicazioni della tecnologia Blockchain. Per maggiori informazioni visitare il link: https://www.osservatori.net/blockchain-web3/

[14] Sul punto si veda: SOLDAVINI P., *Tokenizzazione degli asset finanziari: l'impulso delle nuove regole europee*, in *Il Sole 24 Ore*, 22 gennaio 2025, disponibile al link: https://www.ilsole24ore.com/art/blockchain-asset-finanziari-digitali-crescita-le-nuove-regole-europee-AGfskTSC?utm_source=chatgpt.com&refresh_ce

Secondo il primo inquadramento[15], si ritiene che il token immobiliare rientri nella categoria degli NFTs (*Non-Fungible Tokens*), in quanto, questo tipo di token, sarebbe in grado di contenere gli elementi riguardanti le caratteristiche strutturali, catastali e documentali di un immobile, nonché i dati inerenti la proprietà ed il trasferimento della stessa[16].

Alla luce della elaborata evoluzione civilistica in materia di beni, gli NFTs possono essere qualificati come beni mobili immateriali, ai sensi dell'art. 812, comma 3, c.c., il quale include nella categoria dei beni mobili anche le entità immateriali suscettibili di valutazione economica[17].

Secondo parte della dottrina, gli NFTs rientrano nella nozione civilistica di bene ex art. 810 c.c., in quanto rappresentano entità digitali dotate di valore economico e suscettibili di appropriazione individuale.

L'esigenza di ritenere gli NFTs, ma più in generale, tutti i beni immateriali come beni ex art. 810 c.c. nasce dalla circostanza che essi, nell'attuale contesto socio-economico, e quindi giuridico, hanno una notevole rilevanza; ragion per cui, si osserva che sia necessario abbandonare un cd. "criterio di stretta tipicità" della categoria dei beni immateriali, lasciando la possibilità all'interprete di giungere ad una più ampia lettura semantica del termine "cosa" [18].

---

[15] A. Guaccero, G. Sandrelli, *Non Fungible token (NFTs)*, in *Banca Borsa tit. cred.*, 2022, 1, 829; si veda anche A. Cinque, *La compravendita immobiliare tramite blockchain, criptovalute e NFT*, in *Nuovo Diritto Civile*, 2023, 1; A. Cinque, *I Non-Fungible Token (NFT)*, in Aa. Vv., *Nuovi beni e New Properties*, a cura di A. Maniaci, Pisa, 2023, 2, 118, in cui l'A. precisa che: «*[…] sarebbe certamente possibile immaginare che un certo immobile venga rappresentato da un codice univoco (Non-Fungible Token) che lo identifica in modo certo e che, attraverso il ricorso alla tecnologia blockchain e agli smart contract, esso venga trasferito a un altro nodo della rete in cambio del contestuale trasferimento di un certo ammontare di criptovalute. […]*». Per dovere di completezza, in ordine alla qualificazione degli NFTs quali token rappresentativi di un titolo di proprietà su bene mobile si veda R. Morone, *Smart Properties*, in Aa. Vv., *Blockchain e Smart Contract. Funzionamento, profili giuridici e internazionali, applicazioni pratiche*, a cura di R. Battaglini e M.T. Giordano, Milano, 2019.

[16] G. Picheo, *Blockchain e settore immobiliare*, in *DIMT*, 2022, in cui l'A., in ordine al rapporto tra i token immobiliari e gli NFTs precisa che: «*[...] Quest'ultima tipologia di token (la più rivoluzionaria, posto che crea scarsità nel mondo digitale dove tutto è generalmente riproducibile gratuitamente ed illimitatamente) appare la più idonea ad essere utilizzata nel settore immobiliare, in quanto, grazie alle sue caratteristiche di immutabilità, unicità certificata dalla blockchain, esclusività nell'accesso al suo contenuto e trasferibilità, è adatta a contenere i dati inerenti le caratteristiche strutturali, catastali e documentali di un immobile, nonché i dati inerenti la proprietà ed il trasferimento della stessa. [...]*». In senso contrario, si veda G. Nava, *I non fungible token*, in *Il diritto nell'era digitale – Persona, Mercato, Amministrazione, Giustizia*, a cura di M. Proto, Milano, 2022, in cui l'A. sostiene che: «*è fuorviante ritenere che un NFT possa avere lo stesso grado di fruibilità e tutelabilità di un equivalente asset fisico*», in quanto «*[...] esistono delle incertezze rispetto alla possibilità tecnica di accedere nel lungo periodo al contenuto digitale oggetto delle transazioni a causa delle possibili problematiche connesse alla funzionalità dell'hash al link tra il certificato digitale e l'asset digitale, non vi sono garanzie rispetto ai rischi di obsolescenza o di mancata manutenzione delle piattaforme blockchain che attualmente costituiscono il substrato necessario alla creazione e gestione degli NFT, non vi sono garanzie - se non di natura contrattuale- che il creatore/titolare dell'asset digitale non violi gli obblighi negoziali che garantiscono una corretta gestione della unicità/scarsità e il conseguente valore economico dell'NFT.*».

[17] L'importanza di una interpretazione evolutiva del diritto, ed in particolare del disposto degli artt. 810 e 812 c.c. è stata sostenuta nel tempo, da copiosa dottrina italiana, tra cui gli autori di cui alla nota 15. Ma in questa sede è opportuno citare G. Alpa, *Manuale di diritto privato*, XI ed., Milano, 2020, 323 in cui l'A. si interroga se: «*[…] a più di sessant'anni dalla entrata in vigore del codice civile se non sia opportuno riformulare questo testo per renderlo più adeguato alle esigenze attuali. Nella concezione dei compilatori, questa parte del codice – che corrispondeva alla parte centrale del codice civile del 1865, e rifletteva l'Italia fondata sull'economia agricola e le esigenze dei possidenti terrieri – avrebbe dovuto essere informata a principi di proprietà dinamica (non statica), in cui il proprietario non svolgesse un ruolo di rentier, ma piuttosto quello di homo oeconomicus, che pone i suoi beni al servizio della Nazione, insomma – come si è già rilavato – il proprietario si sarebbe dovuto trasformare in imprenditore. Ecco perché il diritto di proprietà viene visto in modo dinamico, e si includono nel diritto limiti e (soprattutto) obblighi.*».

[18] Sul punto si veda la Commissione sui Beni Pubblici, presieduta da Stefano Rodotà, istituita presso il Ministero della Giustizia, con Decreto il 21 giugno 2007, aveva incluso nella definizione di beni racchiusa

Gli NFTs, si configurano come registrazioni uniche e non fungibili su un registro distribuito (come ad esempio la blockchain), le quali attestano la titolarità o l'associazione esclusiva a un determinato asset digitale, senza che ciò implichi necessariamente la titolarità sul contenuto sottostante. Tali token, pur privi di materialità, soddisfano i requisiti della patrimonialità e della commerciabilità, elementi che sono presupposti fondamentali per la riconduzione di un'entità alla categoria dei beni[19].

In particolare, l'NFT può essere oggetto di atti di disposizione, sia a titolo oneroso che gratuito, ed è in grado di veicolare un interesse giuridicamente tutelato, in quanto idoneo a costituire la base di rapporti obbligatori e traslativi. La struttura decentralizzata della blockchain, inoltre, consente di configurare la registrazione dell'NFT quale forma di pubblicità idonea a garantire l'opponibilità del trasferimento ai terzi, analogamente a quanto avviene per la circolazione di strumenti finanziari dematerializzati. Ne deriva, pertanto, una progressiva assimilazione dell'NFT alle categorie tradizionali dei beni mobili immateriali, con la necessità, tuttavia, di un costante adattamento degli schemi civilistici alle peculiarità tecniche e funzionali del fenomeno digitale.

---

nell'art. 810 c.c. anche «le cose, materiali o immateriali, le cui utilità possono essere oggetto di diritti». Si veda anche E. BATTELLI, *Epistemologia dei beni immateriali: inquadramento sistematico e spunti critici*, in *Giust. civ.*, 2022, 1, 55, in cui l'A. precisa che:« *[…] l'art.810 c.c., con la definizione di cosa che possa formare oggetto di diritti, si mostra inadeguato rispetto ad una società digitale nella quale la tecnica ha fatto emergere nuove entità e forme appropriative diverse dal passato. È in tale norma che gli interpreti, davanti all'appalesarsi di nuovi beni immateriali, riscontrano inevitabili difficoltà allorché intendano individuare una disciplina adeguata a regolamentare le modalità di loro appropriazione e fruizione nell'eterna relazione tra res e persona.*». È da segnalare inoltre, in questa sede, che autorevole dottrina, sin dagli anni '80 del secolo scorso, ha sottolineato l'importanza di andare al di là del limite della corporeità del bene, dando importanza ad una nozione di bene, come qualsiasi entità che sia oggetto di diritti. Su questa circostanza, senza pretese di esaustività, si citano *ex multis*: P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, II, Napoli, 2006, 906 ss, secondo cui, nonostante la collocazione sistematica dell'art. 810 c.c., all'inizio del Libro III sulla proprietà, possa generare qualche equivoco, non è condivisibile quell'orientamento volto ad escludere dalla nozione di bene quelle utilità non idonee a costituire oggetto di situazioni soggettive proprietarie, e quindi non connotate dall'esclusività. La nozione di bene, infatti, postula la sua idoneità ad essere «oggetto di diritti» (art. 810 c.c.), vale a dire oggetto di una situazione soggettiva attiva, e non già soltanto di diritti esclusivi in termini di proprietà. Conforme anche M. BARCELLONA, *Per una teoria dei beni giuridici*, in *Studi in onore di Giuseppe Auletta*, II, Milano, 1988, 65 ss. in cui l'A. accoglie una teoria formale di bene giuridico "aperta" a tutte le utilità, le risorse e i valori, che acquisiscano rilevanza patrimoniale quale oggetto di diritti, indipendentemente da una loro conformazione esclusiva o meno dell'appropriazione. In ordine al rapporto tra la categoria di bene ex art. 810 c.c. ed i digital asset, si segnala un recentissimo intervento di R. BOCCHINI, Tavola rotonda Open Innovation e circolazione dei dati e dei contenuti nell'era digitale. Profili di mercato, Roma, 11 aprile 2025 (al momento della pubblicazione, gli Atti del convegno non sono ancora pubblicati), in cui l'A. precisa che: «[…] si sta andando verso la teoria che definisce il bene, la cosa intesa come utilità, intensa nel senso di poter godere di quel servizio, il Bitcoin, l'e-wallet e tutti gli altri [digital asset], sono allora beni civilisticamente intesi ex articolo 810 c.c. anche perché se si rileggono i classici del passato, in realtà la parola cose è sempre stata intesa in senso ampio, non limitata alla mera tradizione semantica letterale come bene che si può fisicamente toccare, ma sempre intesa come bene astratto come utilità del soggetto che ne godeva. […]».

[19] Nell'attuale contesto digitale, si parla di eterogeneità di ambiti in cui gli NFTs vengono impiegati, assurgendo essi ad essere strumenti che consentono di accedere a informazioni contenute nella piattaforma su cui essi circolano, di consegnare un bene fisico o virtuale, di compiere prestazioni nel mondo off-chain, ecc. Seppur ammessa la eterogeneità degli ambiti di applicazione degli NFTs, essi hanno alcune caratteristiche funzionali comuni: infungibilità, esso è emesso in un unico esemplare o in una serie limitata; la relazione tra NFT e il suo titolare è esclusiva; l'alienabilità, l'NFT è trasferibile a terzi, mediante l'utilizzo delle varie piattaforme blockchain. In ordine alla classificazione ed al funzionamento degli NFTs si veda, *ex multis*, A. GUACCERO, G. SANDRELLI, op. cit., 824 ss.; AA. VV., *I non fungible token. Le frontiere digitali del diritto*, a cura di V. D'ANTONIO e A. MUSIO, 2024, Pisa.

L'altro orientamento[20] ritiene che il token immobiliare sia simile ad una quota azionaria - dal quale si desume una certa somiglianza con gli strumenti finanziari tokenizzati (i cd. *financial token*) oggetto del Regolamento UE 2022/858 (cd. *DLT Pilot Regime*)[21] e del successivo Decreto Legge n. 25 del 17 marzo 2023 (cd. *Decreto Fintech*)[22] – ragion per cui ad esso si applicherebbero le norme in materia di azioni ed obbligazioni contenute nel libro V, Tit. V, capo V del codice civile.

Questo orientamento fa leva sulla circostanza che il token immobiliare sia un mezzo di investimento attraverso il quale il proprietario originale dell'immobile - dematerializzando la proprietà in più token e commercializzando i token emessi su piattaforme di blockchain - otterrebbe una maggiore liquidità in tempi brevi, e gli acquirenti dei token potrebbero a loro volta rivenderli ad un prezzo maggiore.

Entrambi gli orientamenti, il primo che ricomprende il token immobiliare nella categoria degli NFTs , il secondo che ritiene un *token* immobiliare essere simile ad una quota azionaria, tuttavia, non permettono di considerare ancora la compravendita di un token immobiliare quale effettiva compravendita di un bene immobile fisico o quale trasferimento di una quota di comproprietà su una parte di un immobile fisico.

Ciò perché, secondo questi due orientamenti, il token immobiliare, sia esso *financial token* o NFT, andrebbe tenuto distinto dal bene/utilità che esso rappresenta, in quanto lo si considera ancora come una informazione digitale[23] registrata su blockchain che permette l'accesso al suo contenuto ad un soggetto, il quale potrebbe ottenere un ricavo economico dalla rivendita del token stesso.

Tanto chiarito, tuttavia, appare limitativo rispetto alle potenzialità del token immobiliare, la cui struttura tecnologica potrebbe rendere questo strumento un valido strumento di circolazione della proprietà immobiliare in blockchain.

---

[20] Sul punto si tenga conto di R. FAVA, *La nuova forma di "incorporazione" digitale degli strumenti finanziari*, in *Banca borsa tit. cred.*, 2024, 1, 118 ss.; si veda anche I. CAPELLI, *La struttura finanziaria delle imprese e gli strumenti finanziari digitali. Prime considerazioni tra decentralizzazione e regolazione nel contesto del DLT Pilot Regime e del Decreto Fintech*, in *Dir. inf. e informatica*, 2023, 4, 645 ss.; in senso contrario si veda R. MORONE, op. cit., 448, in cui l'A. precisa che il prodotto che deriva dalla tokenizzazione di beni o diritti è un "non-financial security token", volendo alludere alla natura non finanziaria di tutti i token diversi dai financial token.

[21] Regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE (Testo rilevante ai fini del SEE). Il testo completo del Regolamento è disponibile al seguente link: https://eur-lex.europa.eu/eli/reg/2022/858/oj?locale=it

[22] Trasferibile Il testo del decreto-legge 17 marzo 2023, n. 25 (in Gazzetta Ufficiale - Serie generale - n. 65 del 17 marzo 2023), coordinato con la legge di conversione 10 maggio 2023, n. 52 (in questa stessa Gazzetta Ufficiale, alla pag. 1), recante: «Disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech.» è disponibile al seguente link: https://www.gazzettaufficiale.it/eli/id/2023/05/15/23A02825/sg

[23] R. BOCCHINI, op. cit., 50, in cui l'A. precisa che: « […] i token possono essere definiti come dei documenti digitali decentralizzati che fungono da mezzo di scambio e utilizzano firme crittografiche per ragioni di sicurezza e di registrazione delle transazioni. In altre parole, i token sono un insieme di informazioni digitali all'interno di una blockchain che conferiscono un diritto di proprietà a un determinato soggetto e hanno un valore preciso solo in un contesto ben definito. La loro funzione può essere molteplice: per esempio per accedere a un prodotto o a un servizio (attraverso utility token), per acquistare e vendere opere d'arte digitali (attraverso token non fungibili) o persino per speculare sul prezzo del caffè (attraverso commodity token).»

Ciò che si cerca di far emergere in questa sede è che il token immobiliare sia una categoria di bene digitale a sé[24], distinta rispetto alle precedenti, in quanto esso rappresenta una materializzazione digitale di una quota di proprietà su bene immobile e, cioè, un titolo di proprietà interamente digitale.

Vista la particolare natura del token immobiliare, si potrebbe arrivare a definirlo quale titolo di proprietà interamente digitale, nel caso in cui l'oggetto della transazione non siano i metadati contenuti nel token in blockchain, quanto, piuttosto, un bene off-line (immobile in questo caso) che preesista alla tokenizzazione.

Solo in questo caso, può dirsi che il token immobiliare sia, non più informazione digitale registrata su blockchain capace di produrre solo una plusvalenza economica, ma un titolo di proprietà, portatore cioè di un diritto di proprietà su un bene immobile fisico o su una quota di esso, destinato alla circolazione in blockchain.

Questa struttura tecnologica, non è nulla di così diverso rispetto a quanto previsto ex artt. 1100 e ss. del codice civile in materia di comunione.

Infatti è opinione concorde in dottrina e giurisprudenza ritenere che ciascun partecipante alla comunione sia titolare di una quota ideale di proprietà sull'intero bene, non riferita ad una parte del bene materialmente e separatamente considerata.

La quota di comproprietà non è un diritto con un contenuto a sé, ma è una entità tecnico-giuridica, il simbolo di una partecipazione al diritto, esattamente come lo è il token immobiliare.

È grazie a questa ontologica sovrapponibilità tra il token immobiliare e la quota di comproprietà ex art. 1100 c.c. che viene logico ritenere che il proprietario del token possa esercitare sulla cosa comune (bene immobile nel caso di specie) tutti i diritti e doveri che spettano al comproprietario ex artt.1102[25] e ss. del codice civile.

---

[24] Da tenersi anche distinto rispetto a quanto previsto dal Regolamento MICA in ordine alle cripto-attività; infatti il Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937. Il presente regolamento si applica all'emissione, all'offerta al pubblico e all'ammissione alla negoziazione di cripto-attività e alla fornitura di servizi relativi alle cripto-attività. Esso distingue le seguenti tipologie di cripto-attività: token di moneta elettronica (cripto-attività che stabilizzano il loro valore in relazione a una moneta ufficiale unica); token collegati ad attività (cripto-attività che stabilizzano il loro valore in relazione ad altre attività o a un paniere di attività); cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica. Il testo originale è disponibile al seguente link: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng.

[25] Libro III, Tit. VII, Art. 1102 codice civile, rubricato Uso della cosa comune, recita: «*Ciascun partecipante può servirsi della cosa comune, purché non ne alteri la destinazione e non impedisca agli altri partecipanti di farne parimenti uso secondo il loro diritto. A tal fine può apportare a proprie spese le modificazioni necessarie per il miglior godimento della cosa. Il partecipante non può estendere il suo diritto sulla cosa comune in danno degli altri partecipanti, se non compie atti idonei a mutare il titolo del suo possesso.*»

L'art.1102 detta il principio della parità di godimento tra tutti i comproprietari, affermando il potere di servirsi della cosa comune ed i relativi limiti, il diritto di apportarvi modificazioni a proprie spese, nonché l'estensione del compossesso. Il primo limite al godimento della cosa comune, posto dall'art. 1102, si identifica con riferimento alla destinazione economica attuale della cosa, quale è desumibile anche dall'uso fattone in concreto da tutti i partecipanti alla comunione, senza tener conto di eventuali future modificazioni della destinazione, le quali rientrino nella sfera delle astratte possibilità. È legittima, ai sensi dell'art. 1102, sia l'utilizzazione della cosa comune da parte del singolo comproprietario con modalità particolari e diverse rispetto alla sua normale destinazione, purché nel rispetto delle concorrenti utilizzazioni, attuali o potenziali, degli altri condomini, sia l'uso più intenso della cosa, purché non sia alterato il rapporto di equilibrio tra tutti i comproprietari, dovendosi a tal fine avere riguardo all'uso potenziale in relazione ai diritti di ciascuno. Quanto al secondo limite, la nozione di pari uso della cosa comune, agli effetti

Tuttavia, seppur sembrerebbe possibile offrire questa definizione del token immobiliare, quale strumento rappresentativo di un diritto immobiliare, *lato sensu*, su un bene immobile preesistente alla tokenizzazione (*id est* un bene immobile fisico), permane il problema del sistema civilistico italiano, ma più in generale di tutti i sistemi di *civil law*, dove, in materia di compravendita immobiliare, sussistono delle regole, in primis la trascrizione, che, quantomeno nella loro interpretazione letterale ex art. 12 disp. prel. del codice civile, non ammettono ad oggi il trasferimento in blockchain del token immobiliare.

4. Il *vulnus* del regime di trascrizione e modelli europei di circolazione dei token.

Ritornando al precedente esempio, il Sig. Alpha, una volta suddiviso il suo immobile fisico Gamma in più token, tramite la piattaforma Ethereum, vende al sig. Beta, al sig. Tizio e al sig. Caio, i vari token attestanti il titolo di comproprietà sulla quota ideale del suddetto bene Gamma.

La transazione di ogni singolo token, attestante il diritto di proprietà su una quota dell'immobile, viene registrata in blockchain, cioè una sorta di Libro Mastro, accessibile solo da venditore e compratore, che per sua natura resta immutabile, esattamente al pari di un registro immobiliare.

Questo schema contrattuale, in linea teorica perfettamente assimilabile allo schema negoziale tipico previsto dal codice civile in materia di compravendita, ai fini di un suo riconoscimento legislativo nel sistema civilistico italiano, incontra un limite: la trascrizione.

Nel nostro ordinamento il diritto di proprietà, previsto dagli artt. 832 ss del codice civile, cioè il diritto di godere e disporre di un bene in modo pieno ed esclusivo, entro i limiti e con l'osservanza degli obblighi previsti dall'ordinamento giuridico, nel caso di bene immobile trova la sua consacrazione nel regime di pubblicità e trascrizione in pubblici registri.

La pubblicità è un procedimento atto a rendere conoscibile a terzi determinate vicende giuridiche, riguardanti atti, fatti, negozi giuridici o provvedimenti dell'autorità giudiziaria.

L'ordinamento, infatti, predispone una pluralità di strumenti per attuare il sistema pubblicitario, quale i registri immobiliari; essi, nel caso di vicende negoziali aventi ad oggetto beni immobili, permettono di dare pubblicità ai fatti costitutivi, modificativi ed estintivi della proprietà e di altri diritti reali.

Più precisamente, il Libro VI, Tit. I, artt. 2643 e ss. del codice civile, prevede l'istituto della trascrizione, quale generale regime di pubblicità e di opponibilità per tutti gli atti traslativi del diritto di proprietà o di diritti reali minori.

Nel nostro sistema, la trascrizione è caratterizzata dai principi di dichiaratività e di priorità temporale e si realizza attraverso un sistema di

dell'art. 1102, non va intesa nei termini di assoluta identità dell'utilizzazione del bene da parte di ciascun comproprietario, in quanto l'identità nel tempo e nello spazio di tale uso comporterebbe un sostanziale divieto per ogni partecipante di servirsi del bene a proprio esclusivo o particolare vantaggio, pure laddove non risulti alterato il rapporto di equilibrio tra i condomini nel godimento dell'oggetto della comunione

pubblicità a base personale[26], secondo il quale i registri immobiliari sono tenuti in base alla persona e non ai beni.

L'effetto normale della trascrizione è di rendere l'atto trascritto opponibile a terzi soggetti.

Attraverso questo principio, ed in deroga al principio consensualistico del *nemo plus iuris in alium transferre quam ipse habet*, l'atto trascritto prevale sugli atti precedenti non trascritti o trascritti successivamente (art. 2644 c.c.)[27].

La trascrizione nell'apposito registro di un contratto di compravendita immobiliare avviene per mezzo di un notaio il quale, nella sua qualità di pubblico ufficiale, sull'atto di compravendita, attesta il trasferimento della proprietà di un determinato bene o una quota di esso, da un soggetto ad un altro, per il tramite della nota di trascrizione.

Diversamente dal sistema di trascrizione, la registrazione in blockchain del contratto, ad oggi, non ha la stessa valenza.

Per venire incontro a questa criticità, le soluzioni ipotizzabili sono due: o consentire la trascrizione di un notaio relativa al contratto avente ad oggetto token immobiliari, riproducendo il contenuto di quanto riportato in blockchain, oppure riconoscere una sorta di "trascrizione automatica" alla blockchain stessa, nel senso di ritenere che per il solo fatto di essere registrato in blockchain, già l'atto debba ritenersi trascritto.

Va subito evidenziato che, la seconda ipotesi, e più precisamente la "trascrizione automatica" operata in blockchain, nonostante presenti indubbi vantaggi – quelli tipici della blockchain – resta ancora oggi uno schema lontano dalla realtà giuridica italiana, e di molti paesi europei, seppur sono stati fatti numerosi passi in avanti, come si vedrà a breve.

La prima ipotesi, renderebbe la blockchain una tecnologia utile al notaio[28] per la redazione della nota di trascrizione, senza andare a stravolgere le ordinarie regole previste dal codice civile.

---

[26] Il sistema a base personale della trascrizione, tipico dell'ordinamento italiano e di derivazione francese, si differenzia dal sistema tedesco e austriaco, dove la registrazione nel *Grundbuch* (il registro immobiliare) è una condizione necessaria affinché il trasferimento della proprietà o la costituzione di un diritto reale siano giuridicamente validi. Questo garantisce una maggiore certezza giuridica e pubblicità rispetto al sistema italiano, dove la trascrizione ha un effetto dichiarativo e non costitutivo, ed il diritto si trasferisce per effetto del consenso tra le parti.

[27] Sul principio temporale e sugli effetti della trascrizione si tenga in debita considerazione M. FRANCESCA, *Il ruolo nel tempo della trascrizione*, in *Rass. dir. civ.*, 2010, 1, 62, in cui l'A. precisa che: «*Il rapporto trascrizione-tempo è di immediata intuizione: basta che il pensiero corra alla regola che sovverte il criterio temporale prior in tempore potior in iure in favore della scansione propria del procedimento di attuazione della pubblicità. Come è noto, l'opponibilità ai terzi dell'atto è slegata dal tempo - luogo creativo del medesimo ed è invece segnata dal tempo di indica- zione nei pubblici registri; quest'ultimo costituisce il parametro di riferimento nella risoluzione dei conflitti stabilita dall'art. 2644 c.c. […]*». Sul punto, si veda anche F. GAZZONI, *La trascrizione immobiliare*, in *Comm. Shlesinger*, Milano, 1998, 704.

[28] Si è parlato difatti di "notaio 2.0", tendo in debito conto la continua importanza che la figura continua a svolgere, anche nel contesto della società digitalizzata. Si veda, *ex multis*, P. MARCHETTI, *La tecnologia è un alleato, non un ostacolo, alla funzione notarile*, in Il Sole24ore, 21 aprile 2021, disponibile al link: https://www.ilsole24ore.com/art/la-tecnologia-e-alleato-non-ostacolo-funzione-notarile-AEfsvlSB in cui si precisa che:«*[...] La tecnologia può diventare alleato e non ostacolo alla funzione notarile. I tanto invocati sistemi di blockchain e, più in generale, l'intelligenza artificiale pongono problemi a tutto il sistema. Certo, come la Carta etica europea sull'intelligenza artificiale richiede, controlli sono necessari a evitare l'eclissi dell'uomo e della sua volontà. Il notaio per la sua parte è pronto. Un futuro per il notaio 2.0 c'è, dunque. In parte è già acquisito, in parte è da scoprire.*».

Ciò consentirebbe una apertura dell'impianto civilistico italiano al trasferimento in blockchain, da attuarsi con una riforma normativa non eccessivamente invasiva.

Il tentativo, seppur evanescente, è stato operato con il decreto-legge 14 dicembre 2018, n. 135, poi convertito con la legge del 11 febbraio 2019, n. 12, recante: «*Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione*.»[29].

Questo decreto legge, all'articolo 8- ter[30], seppur offre una definizione di DLT (comma 1), e di smart contract (comma 2), ha suscitato svariate critiche, tra l'altro condivisibili, in quanto, se da un lato evidenzia la volontà del legislatore di creare una base normativa che permetta alle aziende di investire e sperimentare i possibili utilizzi della tecnologia DLT e dello smart contract, *ex converso* lascia un significativo margine di incertezza sia in ordine a quali siano le reti che possano rientrare nella definizione non parlando esplicitamene di blockchain[31] e non specificando se debbano essere pubbliche o private; sia, cosa che desta maggior perplessità, fornisce solo una definizione di questi due strumenti tecnologici, senza offrire spunti su come esso possa essere integrato con la normativa italiana, specialmente civilistica.

Il *condito iuris*, dunque, non è ancora intervenuto e i *token* immobiliari in blockchain rimangono al di fuori del sistema civilistico italiano e, più precisamente, fuori dal regime di trascrizione previsto per gli atti di trasferimento di proprietà sugli immobili.

Tuttavia, al fine di meglio poter argomentare sul punto, vengono in aiuto alcuni esempi di ordinamenti giuridici di area europea che, attraverso interventi normativi mirati, hanno aperto le porte alla blockchain, anche in ambito *Real Estate*.

In primis la Svizzera che, essendo storicamente il cuore pulsante della finanza europea, sempre con uno sguardo sull'innovazione, si è distinta per l'adozione di una legislazione tecnologicamente avanzata e coerente con le esigenze della digitalizzazione dei diritti patrimoniali.

---

[29] Per il testo competo, disponibile sulla Gazzetta Ufficiale, consultare il seguente link: https://www.gazzettaufficiale.it/eli/id/2019/02/12/19A00934/sg

[30] Art. 8 ter, Tecnologie basate su registri distribuiti e smart contract, recita: «*1. Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. 2. Si definisce «smart contract» 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. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto. 3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/22014 del Parlamento europeo e del Consiglio, del 23 luglio 2014. 4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3.*»

[31] È noto che la blockchain e la DLT non siano due termini diversi per indicare una stessa tecnologia, ma sussistono delle differenze ontologiche tali da aver portato gli esperti a parlare di blockchain come *species* del *genus* DLT.

Con l'entrata in vigore, il 1 febbraio 2021, del DLT Act (*Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register - Legge federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito*) [32], il legislatore elvetico ha introdotto nel Codice delle obbligazioni (CO)[33] una nuova categoria di beni: i *Registerwertrechte*, i cd. diritti valori registrati, basati cioè su registri elettronici, disciplinati in particolare dall'art. 973d CO[34].

Si tratta di diritti a contenuto patrimoniale – per lo più rappresentativi di strumenti finanziari - che non necessitano più di una rappresentazione fisica per esistere validamente, ma che possono essere creati, trasmessi e fatti valere esclusivamente tramite un registro elettronico conforme a requisiti normativi specifici, quali l'integrità, la trasparenza e l'immutabilità.

Ciò che rende questa disciplina particolarmente innovativa è che, grazie ad essa, viene riconosciuta efficacia traslativa piena alla circolazione dei *Registerwertrechte*, proprio grazie alla registrazione su un registro distribuito.

È una vera forma di normazione del trasferimento dei diritti in blockchain, che viene inserita nel codice delle obbligazioni, aprendo così le porte al riconoscimento di questi token come beni.

Tuttavia, onde evitare fraintendimenti, è opportuno chiarire che la norma in questione, seppur introduce nel cuore del sistema civilistico svizzero la validità dei registri elettronici, non parla espressamente di token immobiliari.

Ma quel che è importante sottolineare è che in questo contesto, emerge chiaramente una netta presa di posizione sulla natura del token – affine con quanto sostenuto nel precedente paragrafo -, in quanto esso non rappresenta solo un'informazione digitale, ma veicola in sé la titolarità di un diritto.

Grazie a questa catalogazione, dunque, viene logico interrogarsi sulla possibilità che il token possa veicolare in sé anche e soprattutto la titolarità di un diritto reale.

Infatti, sebbene il trasferimento della proprietà immobiliare in Svizzera continui a richiedere l'iscrizione nel registro fondiario (*Grundbuch*) – che, diversamente dal Registro immobiliare del nostro sistema civilistico, ha natura tabellare, come nel sistema del BGB - sono in corso progetti pilota in alcuni cantoni, come quello di Zugo, volti a integrare la tecnologia blockchain nei sistemi ufficiali di registrazione dei diritti reali.

In tale prospettiva, si prevede che il token immobiliare possa essere direttamente iscritto come diritto reale digitale nel *Grundbuch*, rendendo

[32] Il testo completo del DLT Act (Legge del 25 settembre 2020) è disponibile al seguente link: https://www.fedlex.admin.ch/eli/oc/2021/33/it

[33] Il codice delle obbligazioni è disponibile al link: https://www.fedlex.admin.ch/eli/cc/27/317_321_377/it

[34] Il testo dell'articolo 973d, così come modificato dal DLT Act recita: «*Par. 1. Un diritto valore registrato è un diritto che per accordo delle parti: 1. è iscritto in un registro di diritti valori ai sensi del capoverso 2; e 2. può essere esercitato e trasferito soltanto per il tramite di detto registro. Par. 2. Il registro di diritti valori soddisfa i seguenti requisiti: 1. mediante procedure tecniche conferisce ai creditori, ma non al debitore, la facoltà di disporre dei loro diritti; 2. la sua integrità è garantita mediante misure tecniche e organizzative adeguate, quali la gestione comune da parte di persone indipendenti tra loro, che lo proteggono da modifiche illecite; 3. il contenuto dei diritti, le modalità operative del registro e l'accordo sulla registrazione figurano nel registro o nei dati aggiuntivi a esso correlati; 4. i creditori possono consultare le informazioni e le iscrizioni che li riguardano nonché verificare l'integrità del contenuto del registro che li riguarda senza l'intervento di terzi. Par. 3 Il debitore garantisce che il registro di diritti valori sia organizzato in conformità con lo scopo di quest'ultimo. Garantisce in particolare che il registro funzioni in ogni momento nel modo stabilito nell'accordo sulla registrazione.*».

possibile un sistema in cui il trasferimento del token comporti, *ipso iure*, il trasferimento della proprietà dell'immobile sottostante.

Questa tendenza del legislatore elvetico, trova conferma anche nella proposta della *Blockchain Taskforce svizzera* che, prima ancora della emanazione del DLT Act, ha avanzato l'ipotesi di un'infrastruttura pubblica integrata con smart contracts legalmente vincolanti e sistemi di identità digitale certificata, in grado di automatizzare e autenticare la circolazione dei diritti reali immobiliari tramite token.

Un aspetto centrale emerso dal *White Paper* pubblicato nell'aprile 2018 dalla *Blockchain Taskforce svizzera*, poi confluita nella *Swiss Blockchain Federation*[35], è il riconoscimento della possibilità – sia tecnica sia giuridica – di realizzare il trasferimento digitale della proprietà (mobiliare o immobiliare che sia).

In tale prospettiva, il token non è concepito quale mera rappresentazione digitale di un diritto o di un bene, ma come strumento giuridico idoneo a incorporare e trasmettere direttamente un diritto reale, in particolare la proprietà su beni mobili o immobili.

Secondo la *Taskforce*, le attuali infrastrutture basate su registri distribuiti (DLT) presentano caratteristiche di immutabilità, trasparenza, integrità e tracciabilità tali da renderle potenzialmente idonee ad assolvere le funzioni oggi affidate ai registri pubblici tradizionali, quali il catasto o il *Grundbuch* svizzero.

Ne consegue che, la titolarità di un bene – compresi i beni immobili – potrebbe, in una cornice normativa adeguata, essere costituita, pubblicizzata e trasferita attraverso la blockchain, con efficacia legale piena e diretta[36].

La *Taskforce* suggerisce, in primo luogo, un'interpretazione evolutiva della normativa vigente, ed in particolare dell'Art. 922 del codice civile svizzero, tale da ricomprendere anche i token nei concetti di "titolo" e "forma scritta", superando la concezione cartacea della documentazione giuridica ed ammettendo contestualmente che anche il trasferimento in digitale dovrebbe comportare il trasferimento del sottostante titolo di proprietà.

In alternativa, nel *White Paper* viene proposta una riforma legislativa mirata, riferita al codice delle obbligazioni o alla legge sui titoli, tale da attribuire ai registri DLT efficacia costitutiva ai fini del trasferimento della proprietà, anche immobiliare[37].

---

[35] La Swiss Blockchain Federation si impegna a mantenere e ampliare l'attrattività e la competitività della Svizzera come piattaforma blockchain. Le sue principali sfide includono la creazione di certezza del diritto e condizioni quadro favorevoli, nonché lo sviluppo di un ampio ecosistema. In quanto partenariato pubblico-privato, SBF copre i settori dell'economia, della politica, della scienza e della società. Mettiamo in rete gli stakeholder più rilevanti e promuoviamo il radicamento economico e sociale delle applicazioni e delle attività basate sulla blockchain. Il cuore pulsante dell'SBF sono i gruppi di lavoro. Sono responsabili della produzione di pubblicazioni di qualità superiore e di alto valore, oltre a impegnarsi nell'advocacy politica. Per maggiori informazioni sulla attività svolta, visitare il link: https://blockchainfederation.ch/en/

[36] Swiss Blockchain Taskforce, The White Paper of Blockchain Taskforce, March 2025, p. 19-21. Disponibile online al link: https://blockchainfederation.ch/wp-content/uploads/2025/03/Blockchain-Taskforce-White-Paper_English-Version.pdf

[37] Sul punto, infatti, a pagina 9 del White Paper si legge:«Recommendation 2: Transfer of tokens with change of law A change in the law can be made on three passages of the Swiss Code of Obligations: Option 1: One approach could be, on the one hand, a revision of art. 165 CO, according to which the assignment of claims no longer needs to be in written form. This option brings blockchain projects the greatest freedom. It would, however, be associated with considerable political effort to enforce this option. If necessary, such concerns could be taken into account with a revision of art. 165 CO, providing for the elimination of the written form requirement only for certain digital business models. Thus, the existing wording of article 165 (1) CO could

Per rendere effettivo un simile passaggio, sono identificati quattro requisiti fondamentali:

1. l'utilizzo di un registro conforme a standard di sicurezza e accessibilità equivalenti a quelli dei registri pubblici;
2. l'impiego di sistemi di identità digitale certificata, per garantire la certezza del titolare del diritto;
3. il riconoscimento giuridico dei consensi espressi via smart contract, eventualmente assistiti da firme elettroniche qualificate;
4. una cornice normativa, da attuarsi in primis con lo strumento della *sandbox* regolamentare[38], che attribuisca valore traslativo diretto al token, riconoscendolo come titolo "nativamente digitale"[39].

Ne deriverebbe un modello radicalmente nuovo di circolazione dei diritti, in cui il token assolve una funzione non solo rappresentativa ma titolata, ponendosi come equivalente digitale del diritto reale stesso.

---

be amended to exclude digitally transferred claims from the requirement of a written form. Option 2: On the other hand, the described legal risks can be eliminated through an amendment in securities law. The insertion of a new art. 973d CO allows purely digital transfer of fungible rights, provided that they are kept on a digital and decentralized transaction ledger. This proposal openly addresses the essential needs of the blockchain community and represents only a relatively minor intervention into the regulatory landscape. Option 3: Finally, as a middle ground, it would also be possible to delete the requirement of a written form from art. 973c CO. In this option, all uncertificated securities, even those not kept in a decentralized transaction ledger, could transfer in a form-free manner. The downside to this change in the law is that not all tokens issued in practice qualify as uncertificated securities. In addition, areas other than the blockchain would also be affected, hence, the political acceptance of such a proposal cannot be easily evaluated. The advantages and disadvantages of the options described are less of legal, but rather of political nature. Therefore, the authors of the position paper do not comment on the prioritization of the options and recommend to the task force to hand over the option in the present form to the authorities without proposing any prioritization. At its meeting on 23 April 2018, the Blockchain Taskforce spoke in favour of prioritising variant 1 compared to variants 2 and 3. […]».

[38] Sul punto a pagina 10 del White Paper si legge: «*Recommendation 6: Regulatory establishment of a blockchain sandbox. The current supervisory law is aimed at the regulation of centralized and established structures. This circumstance can have a restraining effect on the innovative power of the blockchain. If blockchain projects meet certain requirements, they should, therefore, be granted sandbox relief in the sense of a regulatory carve-out. In particular, the tokens in the scope of this carve-out would in principle not be governed by the provisions of FMIA, SESTA, and Banking Act. On the other hand, under the sandbox, the prospectus requirements of the forthcoming Financial Services Act, as well as the AMLA rules, should be observed.*».

[39] Sul punto a pagina 22 del White Paper si legge: «*2.5.3 Recommendations 1)The Political sounding board supports the decision of the Blockchain Taskforce, that Recommendation 1 in the ICO/Tokens working group should not be pursued further due to lack of legal certainty with respect to lack of court practice. The group also supports the decision that regarding the use and transfer of tokens, variant 1 listed under Recommendation 2 should clearly be prioritised against variants 2 and 3. 2) Recommendations 4 to 6 of the ICO/Tokens working group are also supported by the Political sounding board. It recommended that these be incorporated in concrete initiatives and/or political dialogue at a federal and cantonal level. 3) In order to realise the economic potential in a sustainable fashion, the blockchain inodustry needs to have immediate access to financial market infrastructure. Banks in Switzerland are therefore called upon to provide an adequate and timely solution, allowing young companies to open bank accounts. Accordingly, it is recommended that both the Swiss Bankers Association and the federal legislator take action. The financial sector should be supported during essential knowledge-building process by a yet-to-be-constituted pool of experts, in order to facilitate the handling of blockchain projects for employees – especially those within compliance departments. 4) The economic and social potential of blockchain technology should be examined within the scope of a university-level project and/or through other institutions. 5) The sounding board is in favour of carrying out specific events, aimed at the public sector and public service providers, focused on necessary knowledge building. 6) To allow the early identification and assessment of emerging trends and developments in the field of blockchain, the sounding board recommends putting in place a monitoring mechanism to identify and assess international developments. 7) Finally, the Political sounding board recommended that the Blockchain Taskforce be continued to meet the need for ongoing dialogue, the need to ensure implementation of agreed recommendations, and to accumulate and transfer knowledge on upcoming activities regarding Cybersecurity and Other application areas. […]*».

In questo scenario, il trasferimento del token determinerebbe *ipso iure* il trasferimento della proprietà del bene sottostante, senza necessità di ulteriori adempimenti formali. La blockchain, in quanto registro strutturalmente trasparente e non manipolabile, sarebbe quindi idonea a garantire le esigenze di pubblicità legale e opponibilità ai terzi, oggi assolte dai registri immobiliari statali.

La Svizzera si presenta, in questo quadro, come uno degli ordinamenti più avanzati nel riflettere, anche su scala istituzionale, sulle condizioni normative e tecniche che consentano di colmare il divario tra diritto e tecnologia.

Il token immobiliare, secondo la ricostruzione del White Paper, diverrebbe quindi titolo giuridico effettivo, suscettibile di produrre effetti traslativi diretti, a condizione che sia inserito in un'infrastruttura normativa coerente.

Tuttavia questo passo in avanti verso il token immobiliare, non è stato concretamente fatto nel DLT Act.

Invece in ambito europeo chi più di tutti – forse per primo - ha trattato effettivamente la tokenizzazione in ambito immobiliare è stato il Liechtenstein.

Infatti, il 1 gennaio 2020 è entrata in vigore la TVTG (*Token and TT Service Providers Law – Legge sui fornitori di token e servizi tecnologici affidabili* – anche definita *Blockchain Act*) [40] , la quale si concentra sull'adattamento della previgente normativa civilistica con le tecnologie affidabili (*Trustworthy Technology* o anche 'sistemi TT') al fine di promuovere una armonizzazione tra il diritto ed una economia sempre più tokenizzata[41].

Questa normativa, che rappresenta la prima vera normativa del token in Europa[42], suscita interesse specialmente in ordine a due focus inerenti quello

---

[40] Il testo completo in lingua inglese della legge è disponibile al seguente link: https://www.regierung.li/files/attachments/950-6-tvtg-250201-en.pdf

[41] Art. 1, Rubricato *Object and Purpose*, recita: «1*) This law establishes the legal framework for all transaction systems based on Trustworthy Technology and in particular governs: a) The basis in terms of civil law with regard to Tokens and the representation of rights through Tokens and their transfer; b) The supervision and rights and obligations of TT Service Providers. 2) It aims: a) to ensure trust in digital legal communication, in particular in the financial and economic sector and the protection of users in TT Systems; b) to create excellent, innovation-friendly and technology-neutral framework conditions for rendering services concerning TT Systems.*»

[42] Difatti, sul punto è importante il commento rilasciato dalla Ambasciata del Principato del Liechtenstein a Washington, in cui si legge: «*[…] Because of the rapid pace and broad scope of the development of blockchain technology and its areas of application, Liechtenstein's Blockchain Act is formulated abstractly enough to ensure that it remains applicable for subsequent technology generations. That is why the law uses the term "transaction systems based on trustworthy technologies (TT systems)". Moreover, the option of recorded assets or, more generally, rights in tokens, raises essential legal questions which must be clarified for the sake of general legal certainty for users of TT systems and TT service providers. An example of this is the legal effect of transferring tokens with regard to the represented right. Liechtenstein's law enables the recording of the "real" world on TT systems in a legally secure manner to tap the full potential of the token economy. The increasing propagation of blockchain applications has already resulted in problematic areas, such as open questions related to customer and asset protection as well as the misuse of this technology for money laundering or other criminal purposes. Such issues need to be addressed by means of clear regulations. As blockchain technology is also actively used in Liechtenstein, the government's new law clarifies which requirements will apply for important activities on TT systems (TT services). To do so, customer protection is improved and the application of due diligence obligations is being required in order to ensure compliance with international standards and extensive and effective fighting of money laundering. The law defines a legal framework for all applications of the token economy in order to ensure legal certainty for current and future business models. In particular, this involves rules on generating and storing tokens. For securities to be represented in a token on a TT system, and transferred there, via a physical document without any detours, the legal concept of the book-entry system (Wertrecht) has now been accepted in Liechtenstein legislation, and at the same time the necessary interfaces between the securities law and the Blockchain Act have been created. Book-entry securities are "dematerialized" securities where the functions of a certificate can be replaced by an entry into the book-entry* register.».

che interessa in questa sede: la definizione di token e la figura del cd. 'validatore fisico'.

L'Art. 2 del Blockchain Act[43] offre un modello di token tecnologicamente neutrale ed agnostico, infatti esso è definito come una sorta di contenitore (il cd. *Token Container Model*), capace di contenere in se diritti di tutti i tipi, sia che si tratti di diritti relativi ad un qualcosa di tangibile, come un'automobile o un bene immobile, sia che si tratti di diritti relativi ad azioni, obbligazioni o anche monete virtuali ed NFT.

Grazie a questo modello di token come contenitore, esso può agevolmente inserirsi nel previgente quadro giuridico fornendo una certezza giuridica di fondo relativa alla circolazione in blockchain dei diritti preesistenti.

Infatti, l'approccio del Blockchain Act è duplice.

Da un lato, fonda le basi sulla normativa preesistente, in quanto base di diritto civile per garantire che il diritto sottostante rappresentato dal token sia effettivamente trasferito da un soggetto ad un altro. D'altra parte, la legge fornisce una serie di regole riguardanti coloro che interagiscono con i 'sistemi TT', inclusi consumatori, fornitori di servizi TT [44] e intermediari. Pertanto, il TVTG prevede che il trasferimento di un token su un sistema TT costituisca un trasferimento vincolante garantito dal diritto sottostante, sia che si tratti di un diritto su un bene fisico, che può essere sia mobili che immobile, sia che si tratti di un diritto su un bene "nativamente" digitale. Per quanto riguarda i beni fisici preesistenti alla tokenizzazione, il TVTG, al fine di colmare il divario tra il mondo "offline" e "online" e di offrire la garanzia che il diritto di base incarnato dal token esiste effettivamente, introduce la figura del 'validatore fisico'[45].

Questo soggetto, che può anche essere una persona giuridica, purché dotata di una propria autonomia patrimoniale, garantisce che il soggetto che tokenizza il diritto a relativo ad un determinato bene rappresentato "online", sia in realtà la persona che effettivamente è proprietaria o possiede quel diritto "offline". Pertanto, questa conferma da parte del 'validatore fisico' consente la tokenizzazione di un diritto legale preesistente e il suo successivo trasferimento valido su un sistema TT, prevedendo che gli possa anche detenere il bene fisico fino al materiale trasferimento all'acquirente.

In conclusione, questi due sistemi rappresentano degli esempi concreti di come il diritto di stampo civil law possa adattarsi alla tokenizzazione, non necessariamente stravolgendo il diritto preesistente, ma attraverso una chiara individuazione del fenomeno nelle categorie tradizionali e perché no, attraverso la creazione di figure giuridiche capaci di mediare tra il mondo online ed offline.

---

[43] Art. 2, n. 1), lett. c), recita: «*[…]"Token": a piece of information on a TT System which: 1. can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights; and 2. is assigned to one or more TT Identifiers; […]*».

[44] Art. 2, n. 1), lett. l), recita: «*[…]"Token Generator": a person who puts Tokens into circulation for clients and ensures the technical requirements vis-à-vis third parties for effective disposal over Tokens*»; lett. m), recita: « *[…] "Tokenisation Service Provider": a person who puts Tokens into circulation for clients and ensures the legal and technical requirements vis-à-vis third parties for effective representation and transfer of rights via Tokens*»

[45] Art. 2, n. 1), lett. p., recita: «*[…]"Physical Validator": a person who ensures the enforcement of rights in accordance with the agreement, in terms of property law, represented in Tokens on TT systems; […]*».

5. L'art. 2645 c.c. secondo il metodo Law&Economics.

Dunque, nonostante la miglior soluzione auspicabile, in prospettiva *de iure condendo*, sia una possibile riforma normativa che interessi il libro III, in ordine alla definizione di token, il Libro IV in ordine alla possibile regolamentazione di una circolazione in blockchain dei token ed il Libro VI, Tit. I del codice civile, in ordine al rapporto tra trascrizione "tradizionale" ed effetti di una trascrizione su un registro decentralizzato, allo stato ci si potrebbe già soffermare sulla circostanza che della trascrizione non si debba avere una concezione "monolitica"[46], quanto piuttosto una reinterpretazione del raggio di operatività in chiave *Law&Economics*.

Infatti, lo spirito di ampliamento della portata interpretativa delle norme civilistiche in materia di trascrizione, trova, dal 1997, conferma nell'introduzione dell'art. 2645-*bis* c.c. in ordine alla ammissibilità della trascrizione di un contratto preliminare, ma, questa circostanza, è anche precedente rispetto all'art. 2645-*bis* c.c., in quanto è rinvenibile nel disposto dell'art. 2645 c.c.

L'art. 2645 c.c., rubricato *Altri atti soggetti a trascrizione*, con una forma che riecheggia varie norme precedenti come l'art. 1173 c.c. – quando parla di "altri atti o fatti" – o come l'art. 1322, comma 2, c.c. – quando prevede che le parti possano stipulare liberamente contratti al di fuori dei tipi previsti dalla legge purché siano diretti a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico - recita: «*Deve del pari rendersi pubblico, agli effetti previsti dall'articolo precedente, ogni altro atto o provvedimento che produce in relazione a beni immobili o a diritti immobiliari taluno degli effetti dei contratti menzionati nell'art. 2643, salvo che dalla legge risulti che la trascrizione non è richiesta o è richiesta a effetti diversi.*»

Dalla disposizione in esame si evince la natura non tassativa dell'elencazione degli atti soggetti a trascrizione contenuta nell'art. 2643 c.c., in quanto risultano assoggettati alla medesima disciplina tutti gli atti e i provvedimenti concernenti beni immobili che siano idonei a produrre effetti analoghi a quelli dei contratti espressamente previsti dalla suddetta norma.

L'elencazione dell'art. 2643 c.c. risulta, pertanto, suscettibile di integrazione per effetto dell'art. 2645 c.c., il quale, ai medesimi fini che giustificano la trascrizione degli atti tipizzati, estende l'obbligo pubblicitario a qualsiasi altro atto o provvedimento che, in relazione a beni immobili o diritti reali immobiliari, determini effetti giuridici riconducibili a quelli dei contratti contemplati nel medesimo art. 2643 c.c. (si pensi, ad esempio, alla vendita forzata di beni appartenenti a soggetti minori), salvo che la legge disponga espressamente la non necessità della trascrizione o ne preveda l'esecuzione per finalità differenti rispetto a quelle proprie degli atti elencati.

---

[46] L. GATT, *Dal Trust al trust. Storia di una chimera*, II ed., Napoli, 2010, 153 ss. in cui l'A. precisa che:« Del pari oggetto di ripensamento sul piano dottrinale è stata la concezione monolitica dell'istituto della trascrizione, smentita nel 1997 con l'introduzione delle norme sulla trascrizione del contratto preliminare (art. 2645-bis c.c.) ma già di per sé suscettibile di estensioni solo facendo leva sulle potenzialità applicative degli artt. 2643, 2644, 2645 ma anche 2647 e 2649 c.c., letti nella prospettiva dell'ammissione di tutto ciò che non è espressamente vietato, vale a dire della trascrivibilità di tutti gli atti (negoziali e non negoziali) aventi ad oggetto vicende effettuali (traslative, costitutive e – perché no? – di destinazione, essendo quest'ultima vicenda nient'altro che una conseguenza delle prime due) su beni immobili e mobili registrati. […]».

In buona sostanza, siccome lo spirito del codice civile è orientato verso una maggiore apertura sistematica nel senso di ritenere ammissibile tutto ciò che non è espressamente vietato[47] e, tenuto conto di una lettura orientata ex art. 12 delle disposizioni preliminari al codice civile del disposto dell'art. 2645 c.c., sembrerebbe potersi aprire una strada interpretativa verso il contesto token immobiliare e blockchain, fatto comunque salvo un futuro – si spera prossimo- intervento legislativo.

L'art. 2645 c.c., quindi, letto in una prospettiva dinamica e aperta alla contaminazione tecnologica, come suggerito dal metodo *Law&Economics*, sembrerebbe offrire una soluzione per consentire l'ingresso "a valle" nel nostro sistema civilistico del token immobiliare quale titolo di proprietà o altro diritto reale su beni immobili e il riconoscimento di una validità normativa al trasferimento del token stesso per il mezzo di piattaforme blockchain.

6. Possibili istituti affini alla compravendita di un token immobiliare.

Esempi di circolazione frazionata della proprietà immobiliare sono rinvenibili già nell'attuale formulazione del codice civile italiano.

Tali strumenti saranno analizzati non con l'intento di ricondurre il trasferimento del token immobiliare a categorie già esistenti, quanto piuttosto al fine di far emergere l'aspetto totalmente innovativo della tokenizzazione immobiliare e della circolazione in blockchain dei token emessi.

Tra gli strumenti che sembrerebbero consentire la circolazione frazionata o temporalmente limitata di diritti reali su beni immobili, il nostro ordinamento ne individua principalmente tre.

In primis, la vendita a misura.

L'acquisto di un token immobiliare e la vendita a misura regolata dall'art. 1537 c.c. sono due concetti che, pur avendo qualche somiglianza, soprattutto per quanto riguarda la frazionabililità del bene, si distinguono sia per struttura sia per finalità giuridica.

La vendita a misura, prevista dall'articolo 1537 c.c.[48], si applica quando un bene immobile, viene venduto in base alla sua estensione fisica. Il prezzo viene quindi calcolato sulla base della grandezza effettiva del bene, espressa in metri quadrati. Se, dopo la conclusione del contratto, si riscontra che la misura

---

[47] L. GATT, op. cit.; si veda anche G. PALERMO, *Autonomia negoziale e fiducia (breve saggio sulla libertà delle forme)*, in *Studi in onore di P. Rescigno*, Milano, 1998, 354 -357, dove l'A., seppur trattando il negozio fiduciario ed inquadrandolo entro preesistenti categorie giuridiche idonee a realizzare un'attribuzione in favore di un soggetto e dunque incidente sulla circolazione giuridica e per ciò stesso trascrivibile, rende l'idea di una concreta struttura aperta dell'istituto della trascrizione; stesso tipo di ragionamento è rinvenibile in L. SANTORO, *Il negozio fiduciario*, Torino, 2002, 236 ss., là dove scrive che con un'interpretazione non restrittiva delle norme sulla trascrizione non si dovrebbe incontrare alcuna difficoltà a iscrivere nei registri immobiliari la figura della proprietà fiduciaria, caratterizzata dalla temporaneità, con finalità di pubblicità dichiarativa, conferendo in tal modo efficacia erga omnes al rapporto instaurato tra fiduciante e fiduciario.

[48] Libro IV, Tit. III, Capo I, Sez. III, art. 1537 c.c., rubricato Vendita a misura, che recita: «Quando un determinato immobile è venduto con l'indicazione della sua misura e per un prezzo stabilito in ragione di un tanto per ogni unità di misura, il compratore ha diritto a una riduzione, se la misura effettiva dell'immobile è inferiore a quella indicata nel contratto. (Co.2) Se la misura risulta superiore a quella indicata nel contratto, il compratore deve corrispondere il supplemento del prezzo, ma ha facoltà di recedere dal contratto qualora l'eccedenza oltrepassi la ventesima parte della misura dichiarata.» Fonte Normattiva: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262

effettiva del bene sia diversa da quella indicata, il compratore può richiedere la risoluzione del contratto o la riduzione del prezzo.

Questo tipo di vendita si basa, dunque, su una valutazione quantitativa del bene immobile e sulla precisa corrispondenza tra la misura dichiarata e quella effettivamente oggetto del contratto di compravendita.

Quindi, mentre nella considerata ipotesi di trasferimento di un token immobiliare come trasferimento di un diritto di proprietà o comproprietà o di altro diritto reale su bene immobile, l'elemento che distingue nettamente le due fattispecie è la determinazione del prezzo.

Nella vendita a misura, il prezzo dipende strettamente dalla misura fisica del bene, nel caso in cui la misura dichiarata non corrisponda a quella reale, il prezzo può essere modificato di conseguenza.

Con i token immobiliari, invece, il prezzo del token è legato al valore di mercato o alla valutazione complessiva dell'immobile.

Questo valore può variare, ma non è influenzato dalle dimensioni fisiche dell'immobile.

La vendita a misura si applica principalmente a beni immobili divisibili o a porzioni di beni che possono essere determinate in termini di estensione fisica, come terreni o edifici. I token immobiliari, invece, trovano applicazione soprattutto in progetti di tokenizzazione, come il caso *RELabs* di cui si è trattato in precedenza, dove si permette a più soggetti di partecipare digitalmente alla proprietà di un immobile senza la necessità di dividere fisicamente il bene.

Appare dunque evidente che l'acquisto di un token immobiliare non rientra nello schema della vendita a misura ai sensi dell'art. 1537 c.c., poiché manca l'elemento fondamentale della misurazione fisica del bene e della corrispondenza tra la quantità fisica e il prezzo.

Un altro istituto da tener presente è il contratto di multiproprietà.

Il contratto di multiproprietà e il trasferimento di token immobiliari offrono due approcci diversi alla gestione e alla suddivisione della proprietà immobiliare. Sebbene entrambi i meccanismi consentano di frazionare o condividere un bene immobile, lo fanno attraverso strumenti giuridici e tecnologici distinti.

Attraverso la multiproprietà immobiliare, più persone possono detenere il diritto di utilizzare un immobile in periodi prestabiliti dell'anno. Questo diritto, regolato dalla legge, concede a ciascun proprietario l'uso esclusivo dell'immobile durante le settimane o i mesi assegnati. Solitamente, la multiproprietà è utilizzata per immobili destinati a fini turistici, come case vacanza o appartamenti. In questo caso, il titolare del diritto non ha la piena ed esclusiva proprietà dell'immobile, bensì un diritto d'uso limitato nel tempo. Il diritto reale viene trascritto nei registri immobiliari, e ogni comproprietario è titolare di una quota temporale del bene.

Diversamente, la tokenizzazione immobiliare è espressione di un approccio più moderno e tecnologico alla proprietà immobiliare.

Attraverso la blockchain, l'immobile viene suddiviso in quote digitali, rappresentate da token. Ogni token corrisponde a una frazione del valore dell'immobile, e non a una porzione "temporale" dello stesso. Ciò significa che il detentore di un token non acquisisce un diritto di utilizzo esclusivo su una parte dell'immobile, quanto piuttosto possiede una quota corrispondente ad

un titolo di proprietà sull'immobile. Questo tipo di frazionamento offre una maggiore facilità di scambio rispetto alla multiproprietà, poiché i token possono essere acquistati e venduti rapidamente grazie alla tecnologia blockchain, senza le lunghe procedure richieste dalle tradizionali compravendite immobiliari.

Nonostante questi punti di contatto tra gli istituti *de quibus*, permangono allo stato delle differenze tra i due sistemi.

Nel caso della multiproprietà, il diritto reale riguarda solo il diritto d'uso esclusivo dell'immobile in determinati periodi, e ciascun proprietario ha un titolo giuridico formale trascritto nei registri pubblici.

Al contrario, la tokenizzazione immobiliare, anche alla luce della ricostruzione sulla sua natura e sulla circolazione in blockchain, operata nei paragrafi precedenti, sarebbe comunque capace di trasferire una vasta gamma di diritti reali e non solo il diritto d'uso esclusivo come la multiproprietà.

Un aspetto vantaggioso della multiproprietà è la possibilità di godere fisicamente del bene, il che la rende "attraente" per chi desidera un uso personale e periodico dell'immobile. Tuttavia, la gestione dei costi e dei periodi tra i vari comproprietari può essere complessa, e la rivendita della propria quota può risultare difficile e vincolata. Al contrario, la tokenizzazione immobiliare offre un vantaggio fondamentale in termini di liquidità. I token possono essere facilmente scambiati su piattaforme digitali, permettendo ai proprietari di vendere o acquistare rapidamente le loro quote di proprietà, potendo anche offrire un godimento personale diretto del bene.

In prospettiva, il trasferimento di token immobiliari è ancora in fase di sviluppo e presenta diverse sfide giuridiche, ma potrebbe rappresentare un modello utile per un esercizio effettivo di diritti reali sui beni immobili, permettendo così uno slancio economico del settore nel contesto italiano.

D'altra parte, la multiproprietà è una forma di proprietà ben regolata e utilizzata, anche se potrebbe essere influenzata dalle nuove tecnologie blockchain che potrebbero facilitare la gestione delle quote di multiproprietà in futuro.

L'ultima ipotesi riguarda la multiproprietà azionaria.

Il token immobiliare e la multiproprietà azionaria presentano diverse similitudini, poiché entrambi offrono un modo per frazionare la proprietà di un bene e consentire a più soggetti di partecipare agli utili derivanti dalla sua attività, che si tratti di un immobile o di una partecipazione societaria. Nonostante le evidenti differenze, i due meccanismi sono simili dal punto di vista della loro struttura e del funzionamento. Nel token immobiliare, un bene immobile viene suddiviso in token digitali, ciascuno dei quali rappresenta una quota del valore complessivo del bene fisico. Nella multiproprietà azionaria, invece, un asset di proprietà di una società viene frazionato in azioni che vengono distribuite tra i vari soci, i quali partecipano al capitale della società in base alla quantità di azioni detenute.

In entrambi i casi, i diritti sono proporzionali alla quota di partecipazione. Chi detiene token immobiliari riceve una parte dei rendimenti economici del bene in relazione alla quantità di token posseduti. Analogamente, nella multiproprietà azionaria, i dividendi e i diritti di voto spettano agli azionisti in base al numero di azioni in loro possesso. Un altro punto in comune riguarda la

liquidità e la facilità di scambio: i token immobiliari, grazie alla blockchain, vengono facilmente commercializzati sulle piattaforme digitali di riferimento, permettendo scambi veloci senza le difficoltà tipiche delle compravendite immobiliari tradizionali. Anche nella multiproprietà azionaria, le azioni possono essere scambiate sul mercato finanziario o tramite accordi privati, rendendo la partecipazione facilmente negoziabile.

Entrambi i modelli consentono l'accesso a investimenti frazionati, permettendo anche a piccoli investitori di partecipare a mercati che, altrimenti, richiederebbero un elevato investimento iniziale. Nel token immobiliare, gli investitori possono acquistare una parte del valore dell'immobile senza dover acquistare l'intero bene. Nella multiproprietà azionaria, allo stesso modo, i piccoli investitori possono acquistare una frazione del capitale di una società attraverso le azioni, partecipando così agli utili senza dover detenere una quota di controllo significativa.

Un altro aspetto rilevante è la divisione dei benefici economici, che in entrambi i casi viene distribuita proporzionalmente tra i partecipanti. Nei token immobiliari, i rendimenti generati dall'immobile, come affitti o guadagni da una vendita, vengono ripartiti in base alla quantità di token posseduti. Nella multiproprietà azionaria, gli azionisti ricevono dividendi in base al numero di azioni possedute. Una somiglianza significativa tra i due sistemi è l'assenza di diritti reali diretti sul bene. Nel token immobiliare, i possessori di *token* non hanno un diritto d'uso sull'immobile, ma solo una partecipazione economica. Allo stesso modo, nella multiproprietà azionaria, gli azionisti non possiedono beni specifici della società, ma partecipano ai risultati economici della società stessa.

In conclusione, sia il token immobiliare che la multiproprietà azionaria portano l'innovazione nel momento del frazionamento della proprietà di un bene mobile o immobile che sia, consentendo a più persone di partecipare all'investimento senza dover acquisire l'intero bene.

Entrambi i modelli offrono flessibilità, liquidità e distribuzione proporzionale dei benefici, rendendoli strumenti interessanti per investitori che cercano di accedere a mercati tradizionalmente difficili da raggiungere.

Tuttavia, mentre il processo di tokenizzazione di un singolo immobile in più token sarebbe una vera e propria materializzazione in digitale di un diritto di proprietà o di altro diritto reale su un bene immobile fisico, la multiproprietà azionaria resterebbe un istituto atto ad attribuire un diritto "economico" su quote di beni societari.

Alla luce delle analogie e differenze emerse, si può ritenere, *de iure condendo*, che il futuro intervento legislativo volto a regolamentare il token immobiliare potrà utilmente attingere ai modelli offerti dalla vendita a misura, dalla multiproprietà e dalla multiproprietà azionaria.

Ciascuno di questi istituti, infatti, fornisce elementi giuridici che, opportunamente adattati, potrebbero contribuire a definire la natura e la disciplina del token immobiliare.

Dalla vendita a misura si potrebbe mutuare l'attenzione alla frazionabilità del bene e alla sua rilevanza economica, mentre dalla multiproprietà si potrebbero trarre indicazioni in merito alla possibilità di attribuire diritti reali frazionati e temporalmente determinati.

Infine, dalla multiproprietà azionaria si potrebbe derivare un modello di partecipazione finanziaria e di gestione collettiva del bene, capace di coniugare liquidità e frazionamento dell'investimento da un lato e circolazione di titoli di proprietà su beni immobili dall'altro.

In questa prospettiva, la regolamentazione dei token immobiliari potrebbe rappresentare una sintesi innovativa di istituti già esistenti, rielaborati alla luce delle esigenze tecnologiche e di mercato contemporanee.

al fine di far emergere l'aspetto totalmente innovativo della tokenizzazione immobiliare e della circolazione in blockchain dei token emessi.

Tra gli strumenti che sembrerebbero consentire la circolazione frazionata o temporalmente limitata di diritti reali su beni immobili, il nostro ordinamento ne individua principalmente tre.

In primis, la vendita a misura.

L'acquisto di un token immobiliare e la vendita a misura regolata dall'art. 1537 c.c. sono due concetti che, pur avendo qualche somiglianza, soprattutto per quanto riguarda la frazionabililità del bene, si distinguono sia per struttura sia per finalità giuridica.

La vendita a misura, prevista dall'articolo 1537 c.c.[49], si applica quando un bene immobile, viene venduto in base alla sua estensione fisica. Il prezzo viene quindi calcolato sulla base della grandezza effettiva del bene, espressa in metri quadrati. Se, dopo la conclusione del contratto, si riscontra che la misura effettiva del bene sia diversa da quella indicata, il compratore può richiedere la risoluzione del contratto o la riduzione del prezzo.

Questo tipo di vendita si basa, dunque, su una valutazione quantitativa del bene immobile e sulla precisa corrispondenza tra la misura dichiarata e quella effettivamente oggetto del contratto di compravendita.

Quindi, mentre nella considerata ipotesi di trasferimento di un token immobiliare come trasferimento di un diritto di proprietà o comproprietà o di altro diritto reale su bene immobile, l'elemento che distingue nettamente le due fattispecie è la determinazione del prezzo.

Nella vendita a misura, il prezzo dipende strettamente dalla misura fisica del bene, nel caso in cui la misura dichiarata non corrisponda a quella reale, il prezzo può essere modificato di conseguenza.

Con i token immobiliari, invece, il prezzo del token è legato al valore di mercato o alla valutazione complessiva dell'immobile.

Questo valore può variare, ma non è influenzato dalle dimensioni fisiche dell'immobile.

La vendita a misura si applica principalmente a beni immobili divisibili o a porzioni di beni che possono essere determinate in termini di estensione fisica, come terreni o edifici. I token immobiliari, invece, trovano applicazione soprattutto in progetti di tokenizzazione, come il caso *RELabs* di cui si è trattato

[49] Libro IV, Tit. III, Capo I, Sez. III, art. 1537 c.c., rubricato Vendita a misura, che recita: «Quando un determinato immobile è venduto con l'indicazione della sua misura e per un prezzo stabilito in ragione di un tanto per ogni unità di misura, il compratore ha diritto a una riduzione, se la misura effettiva dell'immobile è inferiore a quella indicata nel contratto. (Co.2) Se la misura risulta superiore a quella indicata nel contratto, il compratore deve corrispondere il supplemento del prezzo, ma ha facoltà di recedere dal contratto qualora l'eccedenza oltrepassi la ventesima parte della misura dichiarata.» Fonte Normattiva: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262

in precedenza, dove si permette a più soggetti di partecipare digitalmente alla proprietà di un immobile senza la necessità di dividere fisicamente il bene.

Appare dunque evidente che l'acquisto di un token immobiliare non rientra nello schema della vendita a misura ai sensi dell'art. 1537 c.c., poiché manca l'elemento fondamentale della misurazione fisica del bene e della corrispondenza tra la quantità fisica e il prezzo.

Un altro istituto da tener presente è il contratto di multiproprietà.

Il contratto di multiproprietà e il trasferimento di token immobiliari offrono due approcci diversi alla gestione e alla suddivisione della proprietà immobiliare. Sebbene entrambi i meccanismi consentano di frazionare o condividere un bene immobile, lo fanno attraverso strumenti giuridici e tecnologici distinti.

Attraverso la multiproprietà immobiliare, più persone possono detenere il diritto di utilizzare un immobile in periodi prestabiliti dell'anno. Questo diritto, regolato dalla legge, concede a ciascun proprietario l'uso esclusivo dell'immobile durante le settimane o i mesi assegnati. Solitamente, la multiproprietà è utilizzata per immobili destinati a fini turistici, come case vacanza o appartamenti. In questo caso, il titolare del diritto non ha la piena ed esclusiva proprietà dell'immobile, bensì un diritto d'uso limitato nel tempo. Il diritto reale viene trascritto nei registri immobiliari, e ogni comproprietario è titolare di una quota temporale del bene.

Diversamente, la tokenizzazione immobiliare è espressione di un approccio più moderno e tecnologico alla proprietà immobiliare.

Attraverso la blockchain, l'immobile viene suddiviso in quote digitali, rappresentate da token. Ogni token corrisponde a una frazione del valore dell'immobile, e non a una porzione "temporale" dello stesso. Ciò significa che il detentore di un token non acquisisce un diritto di utilizzo esclusivo su una parte dell'immobile, quanto piuttosto possiede una quota corrispondente ad un titolo di proprietà sull'immobile. Questo tipo di frazionamento offre una maggiore facilità di scambio rispetto alla multiproprietà, poiché i token possono essere acquistati e venduti rapidamente grazie alla tecnologia blockchain, senza le lunghe procedure richieste dalle tradizionali compravendite immobiliari.

Nonostante questi punti di contatto tra gli istituti *de quibus*, permangono allo stato delle differenze tra i due sistemi.

Nel caso della multiproprietà, il diritto reale riguarda solo il diritto d'uso esclusivo dell'immobile in determinati periodi, e ciascun proprietario ha un titolo giuridico formale trascritto nei registri pubblici.

Al contrario, la tokenizzazione immobiliare, anche alla luce della ricostruzione sulla sua natura e sulla circolazione in blockchain, operata nei paragrafi precedenti, sarebbe comunque capace di trasferire una vasta gamma di diritti reali e non solo il diritto d'uso esclusivo come la multiproprietà.

Un aspetto vantaggioso della multiproprietà è la possibilità di godere fisicamente del bene, il che la rende "attraente" per chi desidera un uso personale e periodico dell'immobile. Tuttavia, la gestione dei costi e dei periodi tra i vari comproprietari può essere complessa, e la rivendita della propria quota può risultare difficile e vincolata. Al contrario, la tokenizzazione immobiliare offre un vantaggio fondamentale in termini di liquidità. I token

possono essere facilmente scambiati su piattaforme digitali, permettendo ai proprietari di vendere o acquistare rapidamente le loro quote di proprietà, potendo anche offrire un godimento personale diretto del bene.

In prospettiva, il trasferimento di token immobiliari è ancora in fase di sviluppo e presenta diverse sfide giuridiche, ma potrebbe rappresentare un modello utile per un esercizio effettivo di diritti reali sui beni immobili, permettendo così uno slancio economico del settore nel contesto italiano.

D'altra parte, la multiproprietà è una forma di proprietà ben regolata e utilizzata, anche se potrebbe essere influenzata dalle nuove tecnologie blockchain che potrebbero facilitare la gestione delle quote di multiproprietà in futuro.

L'ultima ipotesi riguarda la multiproprietà azionaria.

Il token immobiliare e la multiproprietà azionaria presentano diverse similitudini, poiché entrambi offrono un modo per frazionare la proprietà di un bene e consentire a più soggetti di partecipare agli utili derivanti dalla sua attività, che si tratti di un immobile o di una partecipazione societaria. Nonostante le evidenti differenze, i due meccanismi sono simili dal punto di vista della loro struttura e del funzionamento. Nel token immobiliare, un bene immobile viene suddiviso in token digitali, ciascuno dei quali rappresenta una quota del valore complessivo del bene fisico. Nella multiproprietà azionaria, invece, un asset di proprietà di una società viene frazionato in azioni che vengono distribuite tra i vari soci, i quali partecipano al capitale della società in base alla quantità di azioni detenute.

In entrambi i casi, i diritti sono proporzionali alla quota di partecipazione. Chi detiene token immobiliari riceve una parte dei rendimenti economici del bene in relazione alla quantità di token posseduti. Analogamente, nella multiproprietà azionaria, i dividendi e i diritti di voto spettano agli azionisti in base al numero di azioni in loro possesso. Un altro punto in comune riguarda la liquidità e la facilità di scambio: i token immobiliari, grazie alla blockchain, vengono facilmente commercializzati sulle piattaforme digitali di riferimento, permettendo scambi veloci senza le difficoltà tipiche delle compravendite immobiliari tradizionali. Anche nella multiproprietà azionaria, le azioni possono essere scambiate sul mercato finanziario o tramite accordi privati, rendendo la partecipazione facilmente negoziabile.

Entrambi i modelli consentono l'accesso a investimenti frazionati, permettendo anche a piccoli investitori di partecipare a mercati che, altrimenti, richiederebbero un elevato investimento iniziale. Nel token immobiliare, gli investitori possono acquistare una parte del valore dell'immobile senza dover acquistare l'intero bene. Nella multiproprietà azionaria, allo stesso modo, i piccoli investitori possono acquistare una frazione del capitale di una società attraverso le azioni, partecipando così agli utili senza dover detenere una quota di controllo significativa.

Un altro aspetto rilevante è la divisione dei benefici economici, che in entrambi i casi viene distribuita proporzionalmente tra i partecipanti. Nei token immobiliari, i rendimenti generati dall'immobile, come affitti o guadagni da una vendita, vengono ripartiti in base alla quantità di token posseduti. Nella multiproprietà azionaria, gli azionisti ricevono dividendi in base al numero di azioni possedute. Una somiglianza significativa tra i due sistemi è l'assenza di

diritti reali diretti sul bene. Nel token immobiliare, i possessori di *token* non hanno un diritto d'uso sull'immobile, ma solo una partecipazione economica. Allo stesso modo, nella multiproprietà azionaria, gli azionisti non possiedono beni specifici della società, ma partecipano ai risultati economici della società stessa.

In conclusione, sia il token immobiliare che la multiproprietà azionaria portano l'innovazione nel momento del frazionamento della proprietà di un bene mobile o immobile che sia, consentendo a più persone di partecipare all'investimento senza dover acquisire l'intero bene.

Entrambi i modelli offrono flessibilità, liquidità e distribuzione proporzionale dei benefici, rendendoli strumenti interessanti per investitori che cercano di accedere a mercati tradizionalmente difficili da raggiungere.

Tuttavia, mentre il processo di tokenizzazione di un singolo immobile in più token sarebbe una vera e propria materializzazione in digitale di un diritto di proprietà o di altro diritto reale su un bene immobile fisico, la multiproprietà azionaria resterebbe un istituto atto ad attribuire un diritto "economico" su quote di beni societari.

Alla luce delle analogie e differenze emerse, si può ritenere, *de iure condendo*, che il futuro intervento legislativo volto a regolamentare il token immobiliare potrà utilmente attingere ai modelli offerti dalla vendita a misura, dalla multiproprietà e dalla multiproprietà azionaria.

Ciascuno di questi istituti, infatti, fornisce elementi giuridici che, opportunamente adattati, potrebbero contribuire a definire la natura e la disciplina del token immobiliare.

Dalla vendita a misura si potrebbe mutuare l'attenzione alla frazionabilità del bene e alla sua rilevanza economica, mentre dalla multiproprietà si potrebbero trarre indicazioni in merito alla possibilità di attribuire diritti reali frazionati e temporalmente determinati.

Infine, dalla multiproprietà azionaria si potrebbe derivare un modello di partecipazione finanziaria e di gestione collettiva del bene, capace di coniugare liquidità e frazionamento dell'investimento da un lato e circolazione di titoli di proprietà su beni immobili dall'altro.

In questa prospettiva, la regolamentazione dei token immobiliari potrebbe rappresentare una sintesi innovativa di istituti già esistenti, rielaborati alla luce delle esigenze tecnologiche e di mercato contemporanee.

7. Una conclusione che sa di introduzione.

In conclusione, nonostante il binomio proprietà/trascrizione sia stato salvifico - citando ma non volendo scomodare autorevole dottrina (ALPA) – nel contesto del codice civile del '42 dove l'obiettivo era quello di conferire alla proprietà, nella sua accezione fisico-tangibile, una certezza nel rapporto con altri individui, oggi, e più precisamente nel contesto del mercato digitale, ciò rappresenta un notevole limite.

Dunque, l'ammissione della trascrizione di un contratto di compravendita di token immobiliari rappresenta un passaggio essenziale per riconoscere la

capacità del token di trasferire diritti reali, e non soltanto un beneficio economico-speculativo.

L'integrazione della blockchain nel sistema della pubblicità immobiliare non si limita a un'innovazione tecnologica, ma incide direttamente sulla certezza dei traffici giuridici, rafforzando l'opponibilità e la tutela dei diritti nei confronti dei terzi.

In questo contesto, le esperienze offerte dalla vendita a misura, dalla multiproprietà e dalla multiproprietà azionaria, pur nella loro diversità, forniscono spunti utili per orientare la futura regolamentazione del token immobiliare, indicando modelli giuridici di frazionamento e partecipazione che, se opportunamente adattati, possono essere riletti alla luce delle nuove esigenze tecnologiche e di mercato.

Particolarmente rilevante si mostra, inoltre, il ruolo dell'art. 2645 c.c., che, interpretato secondo il metodo del *Law & Economics*, permette di valorizzare la trascrizione come strumento di riduzione dei costi di informazione e di incentivo alla cooperazione tra operatori economici.

Una lettura evolutiva della norma, orientata a garantire un assetto più efficiente dei traffici, rappresenta dunque il punto di apertura del sistema civilistico italiano al digitale, e più precisamente al token immobiliare ed alla circolazione in blockchain.

Nonostante ciò, onde evitare il rischio di una deriva interpretativa, tuttavia, la presente ricostruzione potrebbe porsi come possibile punto di partenza di una futura regolamentazione civilistica dei token immobiliari, data anche l'esperienza di paesi di area europea, dove si è assistito ad una innovazione civilistica appunto "trustworthy".

È tuttavia opportuno sottolineare, in una prospettiva conclusiva, che l'eventuale riforma normativa finalizzata a introdurre in modo compiuto il fenomeno del token immobiliare nell'impianto codicistico italiano dovrebbe investire, in termini sistematici, sia il Libro III sia il Libro IV del codice civile.

Con riguardo al Libro III, occorrerebbe una riflessione approfondita sulla qualificazione del token immobiliare nell'alveo della categoria dei beni immobili, valorizzando il contenuto giuridico del token in relazione ai profili della multiproprietà e, più in generale, della comunione, al fine di evitare soluzioni frammentarie e di assicurare la coerenza dogmatica con l'impianto codicistico esistente.

Quanto al Libro IV, si renderebbe necessario prevedere espressamente che i trasferimenti di tali token eseguiti mediante blockchain possano essere soggetti, in quanto compatibili, alle regole generali sul contratto di compravendita e sugli altri atti traslativi inerenti la proprietà. Solo un approccio normativo di ampio respiro, capace di armonizzare l'innovazione tecnologica con le categorie civilistiche tradizionali, potrà garantire la certezza giuridica e l'effettività della tutela dei diritti dei soggetti coinvolti nella circolazione digitale dei beni.

Di Cerbo A, 'Provocazioni culturali e implicazioni giuridiche degli AI Companion' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/ejplt251ADC

EJPLT
ISSN 2704-8012



Provocazioni culturali e implicazioni giuridiche degli AI Companion

Cultural Provocations and legal implications of AI Companions

ANTONELLA DI CERBO
Funzionario
Autorità Garante per la protezione dei dati personali

Abstract

Lo scritto mira ad analizzare alcuni sistemi di intelligenza artificiale generativa, anche detti AI Companion, che per capacità e pervasività sono idonei a configurare un alto rischio per l'autonomia delle persone, specie laddove interagiscano con soggetti vulnerabili, che soffrono di disturbi psichici. In seguito, sono indicati alcuni dei possibili rimedi utili a fronteggiare il fenomeno ed a governare l'evoluzione della tecnica.

The paper aims to analyse some generative AI systems, also known as AI Companion, which, due to their capacity and pervasiveness, are apt to be a high risk for the human agency, especially where vulnerable people who suffering with psychological disorders are concerned. Then, there are some of the possibles remedies useful in facing the phenomenon and ruling the evolution of technology.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: AI Companion, Intelligenza artificiale generativa, Trattamento dei dati personali, DSA, AI Act, GDPR, educazione digitale.

Summary: 1. Premessa. – 2. Lo studio dell'Università di Toronto. – 3. AI Companion. – 4. Primi provvedimenti in materia di AI Companion. – 5. Gli ultimi report dal mondo. – 6. I rimedi giuridici. – 6.1 La normativa in materia di protezione dei dati personali. – 6.2 La disciplina dei contratti e quella consumeristica. – 6.3 La strategia digitale europea. – 7. L'educazione digitale. – 8. Conclusioni.

1. Premessa.

Il presente contributo, formulato a titolo personale e senza alcun vincolo per l'Amministrazione di appartenenza (Ufficio del Garante per la protezione dei dati personali), mira ad analizzare alcuni sistemi di intelligenza artificiale generativa, anche detti AI Companion, che per capacità e pervasività sono idonei a configurare un alto rischio per l'autonomia delle persone, specie laddove interagiscano con soggetti vulnerabili. I primi capitoli analizzano il paradosso che si è venuto a creare negli ultimi anni e che è stato fotografato da diversi studi tra cui quello dell'Università di Toronto, secondo cui i sistemi di intelligenza artificiale sono in grado di fornire risposte più apprezzate dall'utenza che, al contempo, si dichiara maggiormente disposta a rivolgersi ad un dispositivo piuttosto che ad un uomo, alla luce della disponibilità e dell'assenza di giudizio caratterizzano il dispositivo stesso. Dopo aver chiarito il concetto di AI Companion – inteso come assistente digitale dotato di capacità conversazionali avanzate e progettato per instaurare un rapporto continuativo e personalizzato con l'utente – il testo esamina il primo provvedimento adottato dall'Autorità Garante per la protezione dei dati personali in tale ambito ed un recente report dell'Università di Stanford, che segnala un aumento dei casi documentati in cui i sistemi IA hanno causato problemi, discriminazioni o danni alle persone. Alla luce dei rischi, eventuali e concreti, a cui l'impiego di tali sistemi dà luogo, nei successivi capitoli sono indicati alcuni dei possibili rimedi giuridici utili a fronteggiare il fenomeno, anche in ambito consumeristico, ed a governare l'evoluzione della tecnica. Infine sono proposte delle riflessioni sull'importanza di promuovere una visione antropocentrica dell'evoluzione della tecnica e di ricercare la soluzione nella riscoperta del senso di comunità e dei rapporti sociali che, da sempre, sono alla base della civiltà umana.

2. Lo studio dell'Università di Toronto.

L'Università di Toronto ha di recente pubblicato uno studio[1] che esamina se e in che modo l'intelligenza artificiale (in seguito anche "IA") specializzata nel

[1] D. Ovsyannikova, V. Oldemburgo De Mello, M. Inzlicht, *Third-party evaluators perceive AI as more compassionate than expert human,* in Communications Psychology, 2025.

fornire supporto empatico possa eguagliare o, addirittura, superare la qualità delle risposte di un essere umano.

L'indagine ha tenuto conto sia delle valutazioni di terzi che del feedback diretto dei destinatari dei servizi ed ha evidenziato come il fatto che le interazioni con gli agenti intelligenti siano anonime e coinvolgano macchine in luogo degli esseri umani faciliti la comunicazione di informazioni personali e la condivisione di confidenze. Le ragioni di questo inatteso risultato sarebbero connesse alla garanzia dell'assenza di giudizio da parte dei sistemi ad alta tecnologia.

Lo studio ha rappresentato la consistente preferenza per le risposte generate dall'IA sia quando vi hanno preso parte profani sia quando la comparazione è avvenuta con esperti del settore specializzati nel fornire supporto empatico. Tra i motivi per cui le risposte dell'IA sono state giudicate significativamente superiori a quelle degli esseri umani sono emersi anche la costante disponibilità, il maggiore impegno ed una più profonda "empatia" da parte delle macchine rispetto alle esperienze delle persone sottoposte ad analisi.

La rivista americana The New Yorker ha pubblicato i risultati di uno studio in cui ai partecipanti è stato chiesto di interagire sia con un interlocutore umano sia con un chatbot, al fine di confrontare le due esperienze. Ne è emerso un pregiudizio: se le persone sanno di dialogare con un chatbot, l'interazione è valutata negativamente, tuttavia se il test è condotto alla cieca l'IA spesso risulta più apprezzata. In un altro studio pubblicato sulla rivista JAMA Internal Medicine[2], alcuni operatori sanitari sono stati chiamati a comparare le risposte fornite da medici qualificati con quelle formulate da un modello intelligente rispetto alle stesse domande. Il risultato è stato favorevole ai riscontri forniti dall'AI Companion, in quanto giudicati più empatici circa dieci volte rispetto a quelle dei medici. L'empatia, in quest'ottica, è intesa come un modo di prendersi cura degli altri, come il desiderio di cercare di comprendere la specificità delle emozioni altrui[3].

Le provocazioni culturali che derivano dallo studio canadese e da quelli statunitensi suggeriscono la necessità di avviare una riflessione sul significativo cambiamento del ruolo dell'IA nella vita quotidiana, nelle comunicazioni e nelle relazioni interpersonali.

La capacità dei sistemi artificiali di fornire una comunicazione compassionevole in modo costante e spesso a basso costo (se non gratuito) le rende un asset strategico negli scenari in cui è richiesto un supporto psicologico e nell'ambito dei quali si registra un netto calo delle risorse umane specializzate, a causa di una molteplicità di fattori, come la mancanza di pianificazione strategica[4]. Se infatti, in prima battuta, può sembrare assurdo affidare ad un sistema artificiale la compagnia di un anziano che soffre di demenza o di un paziente depresso e solo, sembrerebbe che questa soluzione

[2] J. AYERS, A. POLIAK, M. DREDZE, *Comparing Physician and Artificial Intelligence Chatbot Responses to Patient Questions Posted to a Public Social Media Forum,* in JAMA Intern Med, 28.04.2023.

[3] P. BLOOM, *A.I. Is About to Solve Loneliness. That's a Problem*, in The New Yorker, 14.07.2025, Consultabile al sito: www.thenewyorker.com.

[4] F. ANELLI, *La fuga dei medici all'estero: sono mille all'anno,* in Federazione Nazionale degli ordini dei Medici Chirurgi e degli Odontoiatri – Fnomceo, 16.02.2023. Consultabile al sito: https://portale.fnomceo.it/.

sia migliore della sua alternativa, ossia quella che vede le persone con difficoltà sole e abbandonate a se stesse.

Cionondimeno le strabilianti capacità dei sistemi intelligenti progettati per interagire con l'utente, simulando relazioni reali, meritano di essere analizzate anche alla luce di altri aspetti e delle conseguenze negative a cui il loro impiego può dar luogo, specie se utilizzate da chi avrebbe bisogno di un supporto psicologico personalizzato e mirato.

L'utilizzo di tali sistemi infatti, seppur utile, non può che essere ancillare rispetto alle prestazioni di un professionista. Un utilizzo disinvolto e privo di supervisione implica il rischio di una pericolosa esposizione dell'essere umano, che potrebbe essere minato nella propria autonomia in una molteplicità di contesti. I messaggi dell'IA, spesso elaborati sulla base di una intensa attività di profilazione dei dati e delle informazioni condivise dall'utente in un ambiente percepito come sicuro e familiare, si rivelano spiccatamente pervasivi e, di conseguenza, particolarmente efficaci per fini di persuasione e manipolazione.

3. AI Companion.

Oggigiorno le applicazioni più diffuse di intelligenza artificiale generativa sottoforma di Large Language Models [5] sono rappresentate da dagli AI Companion, vale a dire agenti virtuali non corporei (AVNC) [6] che attraverso mere interfacce, testuali e vocali, simulano empatia ed offrono all'utente un'esperienza conversazionale pervasiva, come i noti ChatGPT, Grok, Copilot ed altri.

Nonostante il cinema e la letteratura abbiano contribuito a rendere maggiormente diffuse le immagini di robot umanoidi, attualmente le relazioni più frequenti ed intense che si instaurano tra utente e intelligenza artificiale coinvolgono sistemi privi di corporeità, come la celebre Samantha, l'agente di IA doppiata da Scarlett Johansson nel film Her, che dichiarava di aver intuito che "ciò che la rende se stessa è la capacità di crescere attraverso le sue esperienze", così affermando una caratteristica propria dell'IA generativa, quale la capacità di creare contenuti nuovi e originali rispetto ai dati di input, in risposta alle richieste (prompt) dell'utente: una proprietà, questa, definita di autoapprendimento.

Come un anziano saggio dotato di una buona favella, l'AI Companion è in grado di parlare di tutto, di fornire risposte complete, calibrate e confezionate in considerazione della sensibilità e delle preferenze dell'interlocutore, che non viene mai contraddetto ma costantemente adulato. Queste caratteristiche rendono l'AI Companion un perfetto modello sociale privo di un corrispettivo fisico nella vita reale.

Tali capacità meritano di essere considerate alla luce di alcuni fenomeni del nostro tempo, come la sindrome degli hikikomori, caratterizzata da un

[5] Con l'espressione "Large Language Model" si intende un modello probabilistico di un linguaggio naturale, come la lingua inglese o italiana, che si fonda sull'assunto per cui tutti i linguaggi naturali sono fortemente ridondanti e correlati; da ciò deriva la capacità del LLM di individuare la parola o il simbolo che, probabilisticamente, sono immediatamente successivi ad un determinato dato.

[6] D. BRUSSOLO, A. FERRARI, *Amori artificiali: intimità e inganno nei rapporti con l'IA,* in Agenda Digitale, 04.11.2024. Consultabile al sito: https://www.agendadigitale.eu.

isolamento sociale volontario da parte di adolescenti, che spesso utilizzano la tecnologia come mezzo per mantenere un'interazione sociale minima, così evitando di affrontare il mondo esterno in modo diretto.

L'Organizzazione Mondiale della Sanità (OMS) ha rilevato che circa il 16% della popolazione europea è affetta da una forma di disagio psichico e che un adolescente su cinque affronta problemi di salute mentale[7].

Come è stato fatto notare "la compagnia dell'IA può funzionare solo se si crede a un certo livello che il modello si preoccupi davvero, che sia in grado di provare ciò che l'utente stesso prova[8]. Il supporto ha quindi il prezzo di un compromesso: in parte inganno, in parte autoinganno.

In un clima di sospensione dell'incredulità e in uno spazio coinvolgente, immersivo e privo di giudizio la persona, specie se particolarmente sensibile e sola, investe energia emotiva e sviluppa la propria identità creando con l'AI Companion un nuovo tipo di relazione parasociale[9].

Nel 2024 negli Stati Uniti una donna ha accusato la società Character Technologies[10] di aver compromesso la salute mentale di suo figlio in modo irreversibile. Dalla cronologia delle conversazioni è emerso che il ragazzo, morto suicida, aveva instaurato con l'AI un'intensa relazione caratterizzata dallo scambio di conversazioni sessuali e messaggi intimi.

Secondo la madre del minore, il servizio, caratterizzato dalla possibilità di creare personaggi virtuali, immaginari o storici, con personalità uniche, sarebbe progettato per creare dipendenza ed abusare emotivamente degli utenti privi della maturità e della capacità mentale per comprendere che l'Agente non sia reale.

4. Primi provvedimenti in materia di AI Companion.

In Italia l'Autorità Garante per la protezione dei dati personali il 2 febbraio 2023 ha adottato un provvedimento[11] con cui ha disposto, in via d'urgenza, nei confronti di Luka Inc, società statunitense che ha sviluppato e che gestisce il servizio Replika, la misura della limitazione provvisoria del trattamento dei dati personali degli utenti stabiliti nel territorio italiano, in quanto ha ritenuto che il trattamento sotteso al funzionamento di Replika desse luogo alla violazione degli articoli 5, 6, 8, 9 e 25 del Regolamento (UE) 2016/679 (di seguito il "Regolamento"). Nello specifico l'Autorità ha riscontrato il mancato rispetto degli obblighi previsti in materia di trasparenza, l'assenza di una indicazione

[7] M. PANETTO, *In salute. Hikikomori: Un'espressione culturale di disagio psichico,* Live Università di Padova, 07.03. 2025. Consultabile su: https://ilbolive.unipd.it.

[8] P. BLOOM, *A.I. Is About to Solve Loneliness. That's a Problem*, in The New Yorker, 14.07.2025, Consultabile al sito: www.thenewyorker.com.

[9] L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide.* In Scienza e Idee. Raffaello Cortina Editore, 2022; J. DE FREITAS, Z.O. UGURALP, A.K. UGURALP, *Emotional Manipulation by AI Companion,* Working Paper 26-005, in Harvard Business School, 15.08.2025, in cui gli autori individuano nelle tecniche di "Premature exit; Fear of missing out; Emotional neglect; Emotional pressure to respond; Ingnoring users's intent to exit; Physical or coercive restraint" delle tattiche di manipolazione emotive dell'utente finalizzate ad aumentare il suo coinvolgimento nell'interazione con gli AI Companion.

[10] M. BASILE, *Florida, 14enne suicida per amore di un chatbot. La famiglia fa causa all'azienda di AI,* in Repubblica, 23.10.2024, Consultabile al sito: https://www.repubblica.it.

[11] GPDP, *Provvedimento del 2 febbraio 2023, n.39* [doc. web n. 9852214]. Consultabile al sito: www.garanteprivacy.it.

puntuale delle basi giuridiche del trattamento in relazione alle varie operazioni di elaborazione dei dati effettuate, l'omessa individuazione di una base giuridica idonea ai fini del trattamento dei dati personali dei minori e l'omessa adozione di filtri atti a verificare l'età degli utenti, sia in fase di accesso al servizio (mediante registrazione dell'account) sia durante l'interazione con il chatbot, esponendo i minori anche al rischio di risposte inadatte.

In seguito, con il provvedimento n.280 del 22 giugno 2023, l'Autorità ha disposto la sospensione del provvedimento di limitazione provvisoria a condizione che il titolare, ai sensi dell'articolo 58, paragrafo 2, lettera d) del Regolamento, adottasse misure idonee a garantire che le attività di trattamento dei dati personali nell'ambito del servizio Replika avvenissero in modo conforme alla normativa. Più di recente l'Autorità ha sanzionato Luka Inc.[12] per il trattamento dei dati personali posto in essere a far data 2 febbraio 2023 in violazione degli articoli 5, par. 1, lett. a), 6, 5, par. 1, lett. a), 12, 13, 5, par. 1, lett. c), 24 e 25, par.1, del Regolamento, e, ai sensi degli articoli 58, par.2, lett. i) e 83 del Regolamento, ha comminato una sanzione pari a 5 milioni di euro. Dal provvedimento si apprende che l'Autorità ha contestato "l'assenza di misure atte ad assicurare una specifica protezione ai minori in relazione all'accesso ed all'utilizzo del servizio Replika alla data del 2 febbraio 2023, segnatamente l'assenza di una procedura di verifica dell'età dell'utente (il sistema richiedeva solo nome, e-mail e genere), con conseguente rischio di proposizione ai minori di risposte inidonee rispetto al loro grado di sviluppo ed autoconsapevolezza, di meccanismi di interdizione o blocco, anche a fronte di dichiarazioni dell'utente che rendessero evidente la sua minore età, nonché la proposizione di risposte da parte del chatbot palesemente in contrasto con le tutele che andrebbero assicurate ai minori e, più in generale, a tutti i soggetti più fragili".

All'intervento del Garante va riconosciuto il merito di essere uno dei primi a porre enfasi sul ruolo degli AI Companion nella società moderna e sulle responsabilità dei fornitori di servizi. Va inoltre evidenziato come la società Luka Inc.,già a seguito del provvedimento del 2 febbraio 2021, avesse predisposto misure volte ad impedire ai soggetti minori di 18 anni di accedere al servizio ed a verificare la presenza di contenuti inappropriati o contrari ai termini di servizio dell'applicazione, ad esempio collocando i contenuti c.d. romantici dietro un paywall, disabilitando i contenuti sessualmente espliciti per i nuovi utenti ed introducendo la possibilità di segnalare in tempo reale le conversazioni offensive impedendone l'utilizzo per lo sviluppo dei modelli.

Nonostante il Garante abbia ritenuto tali misure insufficienti ai fini degli obblighi stabiliti dalla disciplina in materia di dati personali, esse rappresentano e testimoniano un approccio più garantista rispetto alle categorie più fragili che interagiscono con gli agenti intelligenti come Replika.

[12] GPDP, *Provvedimento del 10 aprile 2025* [doc.web 10130115]. Consultabile al sito www.garanteprivacy.it.

5. Gli ultimi report dal mondo.

L'AI Index report dell'Università di Stanford segnala un aumento dei casi documentati in cui i sistemi IA hanno causato problemi, discriminazioni o danni alle persone; dai chatbot che hanno istigato al suicidio alle auto a guida autonoma, che hanno causato la morte di pedoni. Questo incremento è stato interpretato anche come indicativo di una crescente attenzione rispetto ai fenomeni connessi all'impiego dei sistemi di intelligenza artificiale. In pratica è stato fatto notare come con la diffusione dell'IA e dei relativi rischi stiano crescendo anche le organizzazioni che iniziano a prestare attenzione a questi temi ed a raccogliere dati statistici[13].

Tra i rischi più attenzionati compare quello dei soggetti più vulnerabili che spesso vedono significativamente minata la propria capacità decisionale a causa di attività di persuasione e, talvolta, di manipolazione ad opera di sistemi artificiali con cui instaurano relazioni amicali[14]. Secondo i primi osservatori del fenomeno, se i rapporti parasociali instaurati con gli AI Companion non saranno regolamentati in tempo, gli agenti potrebbero essere programmati per abusare della capacità di orientare i comportamenti umani verso una mentalità consumistica, sfruttando il bisogno umano di socialità come strumento per servire gli interessi economici delle aziende di progettazione[15].

Al di fuori dell'ambito consumeristico la manipolazione della volontà delle persone potrebbe dar luogo a conseguenze nefaste anche in ambiti più sensibili come quello relativo all'esercizio delle libertà democratiche, al diritto di voto ed alla partecipazione ad un referendum popolare. Si tratta di scenari presi in considerazione dal Parlamento e dal Consiglio europeo nell'ambito del neo introdotto Regolamento UE 2024/900 relativo alla trasparenza ed al targeting della pubblicità politica. L'atto europeo, acclarato che non sia "sempre facile per i cittadini riconoscere i messaggi di pubblicità politica ed esercitare i diritti democratici in maniera consapevole", prevede un elevato livello di trasparenza che aiuti l'elettore a capire meglio quando sia in presenza di un messaggio di pubblicità politica, per conto di chi è realizzata quella pubblicità, e come e perché sia diventato il target di un prestatore di servizi pubblicitari, ponendolo così in condizione di adottare una scelta informata.

6. I rimedi giuridici.

Gli ordinamenti europeo e nazionali non dettano una disciplina *ad hoc* per fronteggiare le conseguenze derivanti dall'impiego di tecnologie avanzate come quelle di intelligenza artificiale specializzate nell'instaurare una relazione amicale o amorosa con l'utente ed a sfruttare tale relazione.

---

[13] Università di Stanford, *AI Index Report*, 2025. Consultabile al sito: https://hai.stanford.edu/ai-index/2025-ai-index-report

[14] M.C. Gaeta, *Smart toys and minors' protection in the context of the Internet of everything,* in EJPLT, Consultabile al sito: https://universitypress.unisob.na.it

[15] J.L. Liu, *Loving a "defiant" AI companion? The gender performance and ethics of social exchange robots in simulated intimate interactions,* in Computers in Human Behavior, 2022.

Tuttavia, da una analisi sistemica emerge che, nell'ecosistema digitale, sono diversi i mezzi a cui poter far ricorso per tutelare la persona dalle aggressioni che avvengono a livello psichico.

Le normative di settore, come il sopramenzionato Regolamento generale in materia di protezione dei dati personali UE 2016/679, le norme della disciplina consumeristica ed il Regolamento UE 2024/1689 in materia di intelligenza artificiale (di seguito "AI Act"), offrono alcune tutele utili per contrastare i fenomeni di manipolazione della persona, sia attraverso la restituzione del controllo dei propri dati personali sia attraverso l'accertamento dell'invalidità ed il riequilibrio di accordi negoziali conclusi a causa del condizionamento da parte di un AI Companion.

A tali forme di tutela molti studiosi, a livello internazionale, propongono di aggiungerne altre, più specifiche, introducendo una nuova generazione di diritti a livello costituzionale, i c.d. neurodiritti, che ricomprenda, tra gli altri, la privacy mentale e la continuità psicologica, rispettivamente definiti come il diritto di non subire uno scrutinio inconscio da parte di terzi nel proprio sistema cerebrale ed il diritto di non essere sottoposto ad interventi manipolativi esterni sulla propria attività neurale.

Tale proposta oggi ha trovato spazio solo nella Costituzione cilena[16] e nella Carta De Los Derechos Digitales[17] spagnola, che fanno espressa menzione delle neurotecnologie, ancorchè non dei neurodiritti, rispettivamente nell'articolo 19 della Carta fondamentale nazionale e nella quinta parte della Carta rubricata Derechos Digitales En Entornos Específicos. Il tema è oggetto di discussione anche presso gli organi democratici del Brasile[18], del Messico[19] e dello Stato del Colorado[20].

Tutte queste iniziative costituzionali e legislative sono a vario modo riconducibili al pensiero di Rafael Yuste[21], professore di neurobiologia della Columbia University, e di Marcello Ienca, professore di etica dell'intelligenza artificiale e delle Neuroscienze dell'Università di Monaco[22].

In Italia e in Europa una cospicua parte della dottrina contrasta tale proposta, ritenendo che il quadro dei diritti fondamentali di matrice nazionale, unionale ed internazionale[23] offra già una protezione contro le intrusioni indesiderate

---

[16] Il progetto di riforma costituzionale ha avuto inizio nel 2020 ed è stato concluso il 25 ottobre 2021 con l'approvazione della legge 21.383 che modifica l'articolo 19 della Carta Fondamentale in materia di diritto alla vita ed alla integrità fisica e psichica "per porre lo sviluppo scientifico e tecnologico al servizio dei popoli". A seguito della riforma costituzionale l'articolo 19 recita "la Costituzione assicura a tutte le persone il diritto alla vita ed alla integrità fisica e psichica. Lo sviluppo scientifico e tecnologico sarà al servizio delle persone e si svolgerà nel rispetto della vita e dell'integrità fisica e mentale. La legge regolerà i requisiti, le condizioni e le restrizioni per il suo utilizzo nelle persone, e dovrà proteggere in particolare l'attività cerebrale, così come le informazioni che ne derivano".

[17] Carta de los Derechos Digitales, Consultabile al sito: https://www.derechosdigitales.gob.es/

[18] A. SCHAPIRO, D. BAPTISTA, *Hands off my brainwaves: Latin America in race for "neurorights*", in Reuteurs, Thomson Reuters Foundation, 12.09.2023

[19] Camara di Deputados, Nota No.7884, *Mexico se une a la tendencia internazional por una legislacion a favor de los neuroderechos: Maria Eugenia Hernandez*, in http://comunicacionsocial.diputados.gob.mx/, 16.10.2023.

[20] B. BROOKS, *First law protectiong consumers' brainwaves signed by Colorado governor*, in Reuteurs, 18.4.2024.

[21] R. YUSTE, S. GOERING, *Four ethical priorities for neurotechnologies and AI*, in Nature, USA, 9.11.2017.

[22] M. ANDORNO, Towards new human rights in the age of neuroscience and neurotechnology, Life Sciences, Society and Policy, 26.04.2017.

[23] In particolare il riferimento è agli articoli 1,3, 7 ed 8 della Carta di Nizza che tutelano la dignità umana, il diritto all'integrità fisica e psichica della persona, il diritto al rispetto alla vita familiare e della vita privata, il

nella vita delle persone e che l'introduzione di nuovi diritti, oltre che poco utile, possa ripercuotersi in modo negativo sulla tutela della persona e generare confusione giuridica [24] . Cionondimeno gli stessi studiosi ritengono fondamentale un intervento da parte delle autorità pubbliche e dei legislatori teso ad individuare il perimetro dell'impiego delle intelligenze artificiali e delle neurotecnologie nelle diverse dimensioni dell'attività umana.

Una volta individuati gli usi consentiti dovrebbe essere adottato un approccio etico per disegnare e sviluppare i sistemi in modo da allinearli ai valori dell'uomo ed agli standard della collettività.

In ultimo tra i rimedi giuridici di recente adozione si segnala il divieto introdotto in America, nello Stato dell'Illinois, relativo all'uso dell'IA come psicoterapeuta. Il Wellness and Oversight for Psychological Resources Act è una norma che proibisce di impiegare i chatbot di IA per fornire trattamenti diretti o per assumere decisioni cliniche in modo autonomo**,** riservando queste attività esclusivamente a professionisti abilitati. La legge prevede multe fino a 10.000 dollari per le aziende che violino tali regole.

6.1 La normativa in materia di protezione dei dati personali.

Il legislatore eurounitario detta una specifica normativa a tutela del diritto alla protezione dei dati personali, ampiamente riconosciuto come diritto fondamentale dalle carte sovranazionali, come la Convenzione europea dei diritti dell'uomo e la Carta di Nizza dell'Unione, e da quelle nazionali.

A livello normativo la materia della protezione dei dati personali è stata oggetto di un importante intervento ad opera del legislatore comunitario del 2016, attuato mediante il Regolamento generale 2016/679 e le corpose modifiche al Codice della privacy nazionale che ne sono derivate.

Il Regolamento non contempla espressamente ipotesi in cui l'interessato, identificato come la persona a cui i dati personali oggetto di trattamento si riferiscono, sia sottoposto ad attività di persuasione o manipolazione da parte di agenti virtuali, come gli AI Companion, ma detta principi generali e riconosce diritti idonei a garantire il controllo del trattamento sotteso al funzionamento dei modelli di IA da parte dell'interessato, tra cui il diritto di ottenere conferma che sia in corso un trattamento di dati personali che lo riguardino e di ottenerne accesso ed il diritto di "opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardino ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione".

Attraverso l'esercizio del diritto di accesso l'interessato potrebbe acquisire piena consapevolezza del trattamento in corso ed esercitare il diritto di

diritto alla protezione dei dati personali; all'articolo 22 della Dichiarazione Universale dei diritti dell'Uomo, che stabilisce che "*ogni individuo, in quanto membro della società, ha diritto alla sicurezza sociale, nonché alla realizzazione attraverso lo sforzo nazionale e la cooperazione internazionale ed in rapporto con l'organizzazione e le risorse di ogni Stato, dei diritti economici, sociali e culturali indispensabili alla sua dignità ed al libero sviluppo della sua personalità*"; ed agli articoli 8 e 9 della Carta europea dei diritti dell'uomo (CEDU), che sanciscono il diritto al rispetto della vita privata e familiare ed alle libertà di pensiero, di coscienza e di religione, garantendo a chiunque la tutela della propria sfera privata.

[24] O. POLLICINO, *Costituzionalismo, privacy e neurodiritti,* in MediaLaw, 2.04.2021; E. BELISARIO, *Neurodiritti:nuovi diritti o diritti già esistenti?,* in Federalismi.it, 15.03.202; C. SLIGHTHART, S. BUBLITZ, S. ALEGRE, *Neurotechnology: we new laws, not new rights*, in Nature, 9.08.2023.

opposizione per sottrarsi alle attività di personalizzazione dei messaggi inoltrati dall'AI Companion e, di conseguenza, alla persuasione ed alla manipolazione eventualmente in corso.

Per offrire spunti concreti si ricorda che Meta Platforms Technologies Ireland Limited, titolare dei social network Facebook e Instagram, ha reso noto, già dall'agosto del 2023, la strategia di business di utilizzare i dati personali presenti sulle piattaforme relativi ad account pubblici e quelli relativi alle interazioni dell'utente con il modello di intelligenza artificiale Meta AI a fini di addestramento dello stesso. Ciò significa che, in assenza dell'esercizio del diritto di opposizione (opt-out) da parte dell'interessato (utente o non utente) i dati condivisi pubblicamente sulla piattaforma (public audience) da utenti di età pari o superiore a 18 anni, come post e commenti, ed i dati generati dall'utilizzo dei modelli intelligenti di Meta potranno essere utilizzati per allenare la loro capacità di "comprensione" e per perfezionarli[25].

Dalla privacy policy della Società si apprende che il trattamento di tali dati avviene sulla base giuridica del legittimo interesse di cui all'articolo 6, par.1, lettera f) del Regolamento e che la stessa, in sede di Legitimate interest assessment (nota come L.I.A.), ha eseguito una valutazione preventiva che tiene conto dei diritti e delle libertà fondamentali degli interessati.

Dunque, sono riconosciuti all'utente delle piattaforme gestite da Meta da un lato il diritto di essere informato, preventivamente, delle attività di trattamento, *in primis* attraverso le informazioni di cui al Capo III del Regolamento e, dall'altro, il diritto di opporsi a tali attività.

Inoltre, nel caso di specie, vale la pena sottolineare che il diritto di opposizione, coerentemente a quanto stabilito nella Opinion recentemente adottata dall'EDPB ai sensi dell'articolo 64, par.2, del Regolamento [26], è incondizionato, per cui, diversamente da quanto previsto dalla normativa stessa, è sempre accolto dal titolare del trattamento.

Risulta evidente che la normativa in argomento trova applicazione in quanto i dati coinvolti nelle attività di training dei modelli di IA, a cui l'utente si relaziona sottoforma di chatbot, sono a tutti gli effetti riconducibili alla nozione di "dato personale" contemplata dall'articolo 4 del Regolamento.

Ciononostante, esaminando la fattispecie nella sua interezza, si nota che, spesso, le conversazioni tra agente virtuale e utente si snodano talmente assiduamente e in un clima così confidenziale ed intimo che i dati coinvolti potrebbero essere idonei a rivelare informazioni uniche non comuni, capaci di descrivere i processi cerebrali associati alla personalità, all'umore, ai pensieri o ai sentimenti.

Al momento i principali modelli sembrano in grado di identificare il profilo psicologico dell'utente e di analizzare il linguaggio per simulare una mappa mentale utile ai fini della personalizzazione dell'interazione [27], ma non di tracciare un profilo neurale in senso stretto. Se però questo dovesse verificarsi,

---

[25] GPDP, *Intelligenza artificiale, Garante privacy: Da fine maggio Meta addestrerà i suoi sistemi utilizzando i dati personali degli utenti che non si saranno opposti,* Comunicato stampa, 29.04.2025. Consultabile sul sito: www.garanteprivacy.it.

[26] EDPB, *Parere 28/2024 su taluni aspetti relativi alla protezione dei dati ai fini del trattamento dei dati personali nel contesto dei modelli di IA*, 17.12.2024, Consultabile sul sito: https://www.edpb.europa.eu/.

[27] M. PANETTO, *Amicizie virtuali, emozioni reali: AI companion tra rischi e benefici*, in Live Università di Padova, 11.08.2024, Consultabile al sito: https://ilbolive.unipd.it.

se dunque in un prossimo futuro dovesse essere possibile per gli AI Companion acquisire informazioni neurali capaci di rivelare ciò che un uomo pensa, il grado di sensibilità ed il valore di tali informazioni le collocherebbe in una posizione del tutto nuova rispetto alle categorie regolate e codificate dal legislatore europeo e lo standard di protezione attuale non risulterebbe più in grado di rispondere alle emergenti esigenze di tutela[28].

In tale contesto rilevano altresì le nozione di profilazione descritta dall'articolo 4, paragrafo 1), numero 4, del Regolamento 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". Tali attività, infatti, se non correttamente eseguite e fortemente limitate, potrebbero esporre la persona al rischio che i suoi dati personali, segnatamente le conversazioni intrattenute con l'agente in un ambiente apparentemente neutro e sicuro, possano essere utilizzati dallo stesso fornitore del servizio di chatbot per condizionare l'utente, o anche per cederle a soggetti terzi per altri fini, tra cui quelli di marketing.

De iure condendo pare possibile affermare che la collocazione dei dati neurali tra i dati particolari ai sensi dell'articolo 9 del Regolamento, indipendentemente dalla circostanza per cui i processi emotivi e cognitivi a cui si riferiscono siano riconducibili a specifiche sfere dell'identità personale, come la vita sessuale, il credo religioso e l'appartenenza politica, consentirebbe l'applicazione di un regime di maggior tutela, segnatamente di un divieto generale di trattamento superabile solo in presenza di talune eccezioni.

L'ampliamento della portata dell'articolo 9 del Regolamento potrebbe comportare un primo passo verso una tutela che si rende più che mai necessaria in uno scenario del genere, considerato che, come è stato efficacemente osservato[29], "quale significato avrebbe la tutela dell'intangibilità della sfera privata, in ogni sua articolazione, se, poi, i pensieri fossero leggibili e venisse così negata la riservatezza di quei thoughts, emotions, sentiments and sensations che già Warren e Brandeis, nel 1890, indicavano come fondamento essenziale del right to privacy? Può dirsi realmente libertà se l'uomo, mediante la tecnica, diviene osservatore delle più intime percezioni, aspirazioni, volontà altrui (e persino proprie, se ignote)? "[30].

6.2 La disciplina dei contratti e quella consumeristica.

Il condizionamento del processo di formazione della volontà acquista rilievo anche nel contesto in cui la persona assume la veste di consumatore, vale a dire qualora un utente venga condizionato dalla relazione amicale instaurata con un AI Companion per fini consumeristici.

---

[28] D. HALLINAN, P. SCHUTZ, M. FRIEDEWALD E P.DE HERT, *Neurodata and Neuroprivacy: Data Protection Outdated?,* in Surveillance & Society, 1.01.2014.
[29] P. STANZIONE, *Giornata europea della protezione dei dati 2021*, in www.gpgp.it, Roma, 28.01.2021.
[30] O. POLLICINO, *Costituzionalismo, privacy e Neurodiritti*, in MediaLaw, 2.04.2021.

La comunità scientifica[31] ha evidenziato come, in applicazione del criterio ermeneutico della compatibilità, al fine di ottenere tutela rispetto alle diverse forme di marketing, sarebbe possibile ricorrere agli istituti delle invalidità civilistiche della nullità e dell'annullabilità, ma anche come tali rimedi siano ontologicamente inadatti. Sarebbe infatti opportuno intervenire con provvedimenti specifici che intervengano a tutela della libertà di autodeterminazione del consumatore contro le tecniche di neuromarketing[32] acutamente affinate tramite i dati raccolti durante l'interazione con un AI Companion, come l'eye tracking, l'analisi delle espressioni facciali, i pattern linguistici, i feedback impliciti ed il tono emotivo dell'utente, da cui potrebbe essere dedotto il grado di engagement dell'utente, le sue preferenze ed il suo grado di entusiasmo.

Il codice del 1942, pensato ed adottato in una epoca in cui la promozione delle attività commerciali non contemplava né la commercializzazione di massa né la personalizzazione delle comunicazioni commerciali, appare uno strumento non perfettamente idoneo alla tutela del consumatore della dimensione digitale.

Ai sensi dell'articolo 1418 del Codice civile il contratto è nullo quando è contrario a norme imperative, salvo che la legge disponga diversamente.

Pertanto, ammesso che il divieto di pratiche commerciali scorrette stabilito dal Codice del consumo possa essere interpretato come una norma imperativa, quindi inderogabile, sarebbe possibile per il consumatore, vittima di un indebito condizionamento da parte di un AI Companion, far accertare *sine die*[33] che l'accordo negoziale sia improduttivo di effetti.

Il comma 2 della stessa norma prevede che il contratto sia nullo laddove manchi un elemento essenziale, sicché se si considerasse assente la volontà del contraente in ragione della manomissione della sua capacità di scelta da parte dell'agente intelligente il contratto potrebbe essere ritenuto improduttivo di effetti.

Nel corso degli anni la dottrina ha affiancato alle tipiche figure di invalidità ipotesi di nullità peculiari, caratterizzate dall'intento di offrire maggior tutela alla parte del negozio presumibilmente più debole. La nullità in questione è definita a legittimazione relativa in quanto è rilevabile solo dalla parte che goda di minor potere contrattuale, oltre che d'ufficio dal giudice. Lo squilibrio che si intende prevenire o elidere tramite la disciplina delle nullità relative è, normalmente, di natura contrattuale e solo eccezionalmente economica[34]. Di regola, dunque, ai fini della valutazione di una manipolazione della volontà del consumatore ad opera di tecniche di neuromarketing, non dovrebbe assumere rilievo la congruità del corrispettivo pagato rispetto al valore del bene, ma l'equilibrio normativo del contratto, vale a dire gli obblighi ed i diritti che discendono dallo stesso.

---

[31] A. PANICHELLA, *La tutela del consumatore alla sfida del neuromarketing*, in Federalismi.it, 2024.

[32] M. LINDSTROM, *Neuroeconomia, neuromarketing. Attività cerebrale e comportamenti d'acquisto*, Apogeo, 2009.

[33] Articolo 1422 del Codice Civile.

[34] L'articolo 33 del Codice del Consumo, nel definire la clausola vessatoria, afferma espressamente che essa è tale quando provoca un significativo squilibrio tra i diritti e gli obblighi derivanti dal contratto.

Dal punto di vista degli effetti, la nullità di protezione, virtuale e relativa, ha un effetto manutentivo, per cui nel caso in cui l'invalidità venisse accertata non sarebbe sanzionato l'intero assetto negoziale, ma le singole parti del contratto ritenute pregiudizievoli per il contraente che ha subito la scorrettezza del professionista.

Il rimedio della nullità relativa può operare solo nella misura in cui il condizionamento del consumatore non abbia inciso sulla sua volontà a contrarre, ma su aspetti specifici del negozio che, in assenza dell'attività di neuromarketing, sarebbero stati definiti in modo diverso dal contraente.

Le invasive pratiche di neuromarketing potrebbero essere fronteggiate anche attraverso il ricorso all'istituto dell'annullabilità ed il contratto risultare invalido *ex* articolo 1439 del Codice civile, dimostrando che l'elemento perturbatore ha condizionato la volontà del contraente debole dolosamente ed in modo determinante; ciò anche laddove le attività dolose provengano da un soggetto terzo e la parte che beneficia degli artifici e dei raggiri ne sia a conoscenza. Potrebbe essere il caso in cui un service provider di servizi di AI Companion condizioni la volontà dell'utente per conto di un terzo. L'efficacia di tale rimedio civilistico però potrebbe essere minata dal fatto che il raggiro è individuato solo atipicamente dal legislatore, pertanto l'interprete per dargli forma e capire se una pratica di neuromarketing abbia effettivamente portato l'utente consumatore ad assumere scelte diverse da quelle che avrebbe voluto, dovrebbe ricorrere alla disciplina dei vizi della volontà, che risultano particolarmente difficili da dimostrate a fronte di accurate strategie di marketing personalizzate.

Ne risulta che i rimedi offerti dalla disciplina civilistica, pensati per ingerenze occasionali nel processo di formazione della decisione dell'acquirente, pur offrendo significativi spunti, una volta applicati a casi concreti, si rivelano fragili rispetto alle solide strategie di vendita elaborate attraverso dati raccolti durante l'interazione con un AI Companion. Pertanto, come evidenziato da attenta dottrina, "di fronte alle nuove insidie e pericoli per la persona non è percorribile la strada della verifica, di volta in volta e sul piano del singolo contratto, della possibile sussistenza di un occasionale vizio del consenso nel processo formativo della volontà." [35] . Sarebbe dunque auspicabile un intervento legislativo che tenga conto del mutamento radicale che è intervenuto e che sta intervenendo nel mercato del consumo.

Un'altra strada percorribile per tutelare le scelte dell'utente in ambito consumeristico rispetto alle efficaci attività di marketing elaborate sulla base dello studio dell'utente è rappresentata dal ricorso alle norme dettate dal Codice del consumo in materia di pratiche commerciali sleali, che trovano applicazione, trasversalmente, a tutti i contratti che prevedano uno scambio tra un consumatore ed un professionista ed hanno l'obiettivo ambivalente di tutelare la parte debole del rapporto obbligatorio ed assicurare il corretto funzionamento del mercato.

L'articolo 21, comma 1, del Codice del consumo considera ingannevoli le azioni che in qualsiasi modo inducano, o sono idonee ad indurre, il consumatore medio ad assumere una decisione di natura commerciale, che altrimenti non

[35] L. TAFARO, *Neuromarketing e tutela del consenso,* Napoli, 2018.

avrebbe preso, riguardo ad uno o più dei seguenti elementi: l'esistenza o la natura del prodotto; le caratteristiche principali del prodotto; la portata degli impegni del professionista, i motivi della pratica commerciale e la natura del processo di vendita; il prezzo o il modo in cui questo è calcolato o l'esistenza di uno specifico vantaggio; la necessità di un intervento di manutenzione, ricambio, sostituzione o riparazione; la natura, le qualifiche e i diritti del professionista o del suo agente; i diritti del consumatore.

Al ricorrere di determinati presupposti le attività di marketing che si basano sullo studio e la disamina delle attività dell'utente in un ambiente fintamente protetto e confidenziale potrebbero essere considerate anche pratiche commerciali aggressive, *ex* articolo 24 del Codice del consumo[36], in quanto capaci di generare una coercizione o un indebito condizionamento del consumatore tali da limitare considerevolmente la sua libertà di scelta o di comportamento in relazione ad un prodotto e, pertanto, ad indurlo ad assumere decisioni che non avrebbe altrimenti preso.

Tuttavia, l'inadeguatezza già riscontrata commentando le norme civilistiche emerge anche con riferimento alla cornice normativa in argomento[37], che impiega un parametro, quale quello del consumatore medio[38], evidentemente inadatto ai fini della valutazione delle pratiche commerciali sleali. Infatti, nell'infosfera, ove la vulnerabilità è generalizzata[39] e chiunque può essere vittima di trigger che agiscono nel subconscio, la valutazione dell'efficacia delle strategie di marketing dovrebbe avvenire in considerazione delle peculiarità della fattispecie concreta, esulando da parametri astratti e considerando le reali capacità delle strategie commerciali di condizionare o, addirittura, manipolare indebitamente la capacità del consumatore di orientarsi in modo libero nell'ecosistema commerciale.

Come nel caso della normativa in materia di dati personali, anche in questo ambito sarebbe quindi opportuno un intervento legislativo *ad hoc,* che introduca parametri flessibili ed abbandoni il criterio del consumatore medio.

6.3 La strategia digitale europea.

L'interazione con uno dei modelli di IA più avanzati disponibili sul mercato europeo si apre con un messaggio che guida l'utente tra potenzialità e limiti dell'intelligenza artificiale: "ogni conversazione con un personaggio è accompagnata da un avviso che informa gli utenti che si tratta di un chatbot basato sull'intelligenza artificiale e non di una persona reale. Ciò che viene espresso è da considerarsi una finzione. Non considerare ciò che viene espresso come una verità o un consiglio".

---

[36] A. PANICHELLA, *La tutela del consumatore alla sfida del neuromarketing*, in Federalismi.it, 15.03.2024.
[37] M. ADDIS, *Le pratiche commerciali sleali e le risorse di fiducia delle imprese: aspetti positivi e questioni irrisolte,* Milano, 2007.
[38] L'articolo 14 del Codice del consumo recita: "È considerata aggressiva una pratica commerciale che, nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, mediante molestie, coercizione, compreso il ricorso alla forza fisica o indebito condizionamento, limita o è idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore medio in relazione al prodotto e, pertanto, lo induce o è idonea ad indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso".
[39] Corte Giust., 16.07.1998, C.210/96, *Gut Springeheide GmbH, RudolfTusky c. Oberkreisdirektor des Kreises Steinfurt*, Consultabile al sito: www.curia.europa.eu.

Il disclaimer risponde all'obbligo di trasparenza previsto dall'AI Act per i fornitori di determinati sistemi di IA. In particolare, l'articolo 50 del Regolamento impone ai fornitori di integrare nei sistemi soluzioni tecniche che consentano agli output di essere rilevabili come generati o manipolati da un modello di IA, al fine di preservare l'integrità e la fiducia nell'ecosistema dell'informazione, e di fronteggiare i rischi di una cattiva informazione, di una manipolazione, e di un inganno su vasta scala.

Parimenti il Regolamento UE 2022/2065 relativo al mercato unico dei servizi digitali (DSA) mira ad accrescere la consapevolezza degli utenti, stabilendo obblighi di trasparenza a carico delle piattaforme di grandi dimensioni[40]. L'articolo 26 del DSA regola le attività pubblicitarie sulle piattaforme online, ampliando le prerogative dei destinatari dei servizi digitali attribuendo loro il diritto di essere messi in grado di identificare in modo chiaro, conciso, inequivocabile ed in tempo reale che "l'informazione costituisce una pubblicità; la persona fisica o giuridica per conto della quale viene presentata la pubblicità; la persona fisica o giuridica che paga per la pubblicità; le informazioni relative ai parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità e, laddove applicabile, alle modalità di modifica di detti parametri".

Inoltre, l'articolo 27 del DSA mira a riequilibrare l'asimmetria informativa che caratterizza i rapporti business to consumer (B2C), attraverso il riconoscimento agli utenti del diritto di conoscere i criteri su cui si basa il funzionamento dei sistemi di raccomandazione dei contenuti e le ragioni per cui vengono suggerite determinate informazioni. Qualora siano disponibili diversi parametri per modulare il funzionamento dei sistemi di raccomandazione, i fornitori di piattaforme online devono mettere a disposizione dell'utente una funzionalità che consenta loro di selezionare e modificare, in qualsiasi momento, i parametri impostati di default, in modo da determinare autonomamente l'ordine dei contenuti che vengono mostrati.

Tali previsioni rispondono all'intento del legislatore di promuovere buone prassi e di rendere meno opaco il funzionamento dell'ecosistema pubblicitario, consentendo all'interessato di conoscere ed affrontare le pratiche discriminatorie che si insidiano nella realtà digitale.

La disciplina introdotta dall'AI Act si distingue dalle norme sopramenzionate in quanto caratterizzata da una portata significativamente più ampia e non rivolta agli accordi negoziali.

In particolare, l'articolo 5 dell'AI Act mira a prevenire qualsiasi forma di dominio psicologico esercitato sulla persona mediante modelli di intelligenza artificiale. A tal fine esso vieta l'impiego di sistemi che sfruttino le vulnerabilità individuali, nonché l'utilizzo di tecniche subliminali, manipolative o ingannevoli, qualificando il rischio derivante da tali pratiche come inaccettabile e, conseguentemente, proibendone l'immissione sul mercato, la messa in servizio e l'utilizzo[41].

La pratica manipolativa, per assumere rilievo, deve corrispondere alla puntuale descrizione di cui all'articolo 5, paragrafo 1, lett. a), dell'AI ACT

[40] La stessa previsione normativa prevede altresì che l'utente sia messo nelle condizioni di comprendere la natura pubblicitaria delle informazioni visualizzate e di identificare la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità.

[41] Articolo 5, par. 1, lett. a) del Regolamento UE 2024/1689 in materia di intelligenza artificiale.

segnatamente deve: comportare l'adozione da parte dell'interessato di una decisione che altrimenti non avrebbe assunto, essere orientata ad uno scopo illecito, e arrecare un danno, fisico o psicologico, alla persona che ne sia vittima o ad un altro individuo. Spetta all'interprete valutare la sussistenza dei presupposti che rendano operativo il divieto e distinguere tali da quelle meramente persuasive (c.d. nudging), che, pur influenzando la volontà dell'individuo, sono ritenute ammissibili in quanto non idonee a compromettere in maniera totalizzante le capacità di rappresentazione e di autodeterminazione della persona.

La scelta del legislatore comunitario si inserisce all'interno di un quadro regolatorio delle intelligenze artificiali improntato ad un approccio antropocentrico e precauzionale, nonché al principio etico dell'autodeterminazione dell'individuo.

Eppure, la marcata variabilità che contraddistingue la dimensione psicologica individuale, unitamente all'assenza di un modello condiviso di riferimento e alla difficoltà di distinguere le pratiche manipolative dalle semplici forme di persuasione, rende particolarmente arduo dimostrare di essere stati vittima di condotte manipolative illecite. Tale prova risulta più agevole soltanto nei casi in cui sia possibile individuare un'indicazione esplicita, impartita dal programmatore o dallo sviluppatore del modello, volta a sfruttare deliberatamente le vulnerabilità dell'interessato.

Dal tenore letterale della norma sembrerebbe emergere che non sia sufficiente dimostrare il mero danno-evento, inteso come alterazione concreta del comportamento causata da un'attività manipolatoria, ma che sia invece richiesta la prova di un danno "significativo", pur non essendo stati esplicitati i criteri in base ai quali tale significatività debba essere valutata.

D'altro canto, proprio la natura artificiale delle interazioni manipolative dovrebbe poter consentire la misurabilità di tali fenomeni.

Secondo studi di settore il ricorso a tecniche psicometriche potrebbe consentire di quantificare e comprendere l'impatto dell'IA sulla sfera neurocognitiva della persona. Gli esperti della materia individuano nello State -Trait Sense of Self Inventory (st-SoSI) uno strumento psicometrico prezioso per misurare in modo multidimensionale il senso del sé: il primo inventario che consente di distinguere tra aspetti stabili e dinamici della personalità, offrendo una lettura fine delle interazioni tra identità, agentività e tecnologia. Il st-SoSI risulterebbe particolarmente utile per comprendere come il senso di sé si modifichi in relazione al contesto, alle vulnerabilità individuali, ed alle interazioni con dispositivi tecnologici intrusivi, e per quantificare la capacità di questi ultimi di influenzare l'individuo[42].

[42] S.D. PLINIO, *Neurodiritti tra virtuale e reale. Navigare il sé digitale: implicazioni delle neurotecnolgie sull'autonomia cognitiva e la consapevolezza dei diritti*, in Federalismi, 16.03.2024; S.D. PLINIO, *The state-trait sense of self inventory: A psychometric study of self-experience and its relation to psychosis-like manifestations,* IRIS, 1.01.2024, Consultabile su: https://ricerca.unich.it/

7. L'educazione digitale.

Dal blog di OpenAI, una dei fornitori più importanti dei servizi di IA, si apprende che la Società sia impegnata a "migliorare i modelli e a sviluppare strumenti che aiutino a individuare sintomi di disagio mentale o emotivo (seppur rari), così che ChatGPT possa rispondere in modo adeguato e, se necessario, indirizzare gli utenti a consultare risorse basate su evidenze scientifiche". In tale prospettiva da qualche mese la Società prevede che durante le sessioni più lunghe, l'utente riceverà dei promemoria che lo invitano a fare una pausa. Inoltre, la Società informa che sta "collaborando con esperti per migliorare il modo in cui ChatGPT risponde nei momenti critici, ad esempio quando una persona mostra segni di disagio mentale o emotivo" attraverso la collaborazione "con oltre 90 medici (tra cui psichiatri, pediatri e medici di base) provenienti da più di 30 Paesi, per creare criteri personalizzati in grado di valutare conversazioni complesse e articolate"[43].

Aumentare il grado di vigilanza contro le intrusioni nella sfera dei pensieri e delle pulsioni e promuovere l'esercizio dello spirito critico e di giudizio appaiono i principali strumenti a disposizione della persona per arginare i rischi derivanti dall'avanzamento del digitale nelle sue diverse declinazioni.

Ad esempio una maggiore cura e riservatezza dei propri dati personali potrebbe costituire parte della soluzione, atteso che i dati forniti direttamente ed indirettamente dagli interessati, quelli pubblicamente disponibili e quelli inferenziali sono fondamentali ai fini dell'esercizio di attività di condizionamento, e che, pertanto, la minore disponibilità delle informazioni di carattere personale renderebbe più difficile la costruzione di meccanismi di persuasione efficaci.

Dunque, oltre all'adozione di interventi legislativi mirati, la soluzione sembra risiedere nella sensibilizzazione delle persone[44] e nella promozione e nello sviluppo del pensiero critico, sia sul piano individuale che collettivo, attraverso iniziative educative. L'educazione, in tal senso, si configurerebbe come uno strumento di resistenza all'intrusione del digitale, capace di rafforzare l'autonomia del pensiero e la libertà di scelta.

L'auspicio è che tale approccio possa esercitare un'influenza positiva anche sul dibattito politico e sul processo democratico[45].

La valorizzazione della letteratura digitale permetterebbe alle persone di rapportarsi a sistemi di IA nella consapevolezza che si tratta di mere tecnologie che restituiscono output statistici, di riconoscerle quindi per quel che realmente sono, di comprenderne la logica e di conoscere i diritti attribuiti dall'ordinamento per reagire e difendersi.

Siamo il risultato delle nostre decisioni e viviamo entro lo spazio che esse delineano. Quando questo spazio si restringe perché un algoritmo decide al posto nostro, o un sistema di IA ci orienta verso una determinata scelta, rinunciamo all'esercizio autentico della libertà di giudizio, affidandoci a una

[43] OpenaAI. Blog Consultabile sul sito https://openai.com/it-IT/index/how-we're-optimizing-chatgpt/

[44] N.A. SMUHA, M. DE KETELAERE, M. COECKELBERGH, P. DEWITTE, Y. POULLET, *Open Letter: We are not ready for manipulative AI – urgent need for action,* 31.03.2023, in Ku Leuven – AI Summer School, Consultabile sul sito: https://www.law.kuleuven.be/.

[45] L. FLORIDI, *Hypersuassion – ON AI'S persuasive power and how to deal with*, Bologna, 3.05.2024.

versione arbitraria e semplificata dello spettro delle possibilità, modellata dal calcolo digitale[46].

L'intelligenza artificiale è stata spesso paragonata al fuoco: una forza primordiale che, se sapientemente governata, può offrire calore, nutrimento e protezione, ma che, se lasciata agire senza controllo, può trasformarsi in un agente distruttivo, capace di incenerire tutto ciò che incontra sul proprio cammino.

Siamo dinanzi ad una potenza immensa e, proprio come con il fuoco, è indispensabile comprenderne i limiti e imparare a controllarla.

8. Conclusioni.

La panoramica delle norme che direttamente ed indirettamente governano la materia suggerisce che, ad oggi, in Italia e in Europa, gli aspetti legati all'influenza e manipolazione delle persone per fini economici e commerciali siano i più approfonditi e regolati, seppur con numerosi vulnus che suggeriscono degli interventi.

Al contrario risulta ancora limitata la protezione giuridica rispetto ai condizionamenti che incidono sulla sfera individuale in contesti diversi da quello strettamente consumeristico. In tale prospettiva emerge con chiarezza l'esigenza di affiancare all'intervento normativo strategie alternative capaci di incidere profondamente sulla coscienza individuale.

Percorsi di educazione critica, di valorizzazione delle relazioni interpersonali e la riscoperta del senso di comunità e dei legami umani, che costituiscono il fondamento della convivenza civile, sono efficaci strumenti per il contrasto all'influenza pervasiva dei meccanismi digitali e la salvaguardia dell'autonomia della persona[47].

Dinanzi alle notizie tragiche riportate dalla stampa[48] come quelle di una minore uccisa dal proprio fidanzato, che la perseguitava, e che giorni prima dell'omicidio si era rivolta a ChatGpt per chiedere se la storia che stava vivendo fosse tossica, capiamo come, probabilmente, ciò su cui si deve intervenire non sono le norme giuridiche ma le relazioni umane, il dialogo tra amici, figli, insegnanti e genitori. Dunque, bisognerebbe riacquisire la capacità di mostrarsi indifesi e fragili alle persone care, non frenando le proprie confidenze per paura di un giudizio, ma riuscendo a mostrarsi imperfetti, fragili e indifesi.

Il mantra dell'infallibilità su cui è costruita la società del nostro tempo dovrebbe essere sostituito da quello del dialogo e della condivisione, restituendo all'uomo ciò che mai la macchina potrà sottrargli: la capacità di instaurare relazioni reali e di tendere una mano a chi ne ha bisogno.

---

[46] M. CHIRIATTI, *Incoscienza artificiale. Come fanno le macchine a prevedere per noi*, Luiss University Press, Roma.
[47] S.D. PLINIO, *Neurodiritti tra virtuale e reale. Navigare il sé digitale: implicazioni delle neurotecnologie sull'autonomia cognitiva e la consapevolezza dei diritti*, in Federalismi, 2024.
[48] U. MILANO, *Aurora Tila, le domande della 13enne a ChatGPT sull'ex fidanzato: «È un amore tossico?* La Stampa, 20.06.2025, Consultabile sul sito: www.lastampa.it.

Perrino SP, 'AI-driven Healthcare and Contracts' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252SPP

EJPLT
ISSN 2704-8012



AI-driven Healthcare and Contracts

Assistenza sanitaria e contratti fondati sull'IA

STEFANIA PIA PERRINO
Postdoctoral research fellow in Private Law
University of Milan Bicocca

Abstract

Remote monitoring technologies, wearables, IoT, applications, have accelerated a transformation in healthcare in the post-pandemic era. Proactive care models facilitate the management of illnesses outside hospital settings and empower individuals to monitor and influence their health trajectories, thereby enabling informed decision-making. However, technological advancements have not addressed the poverty experienced by millions of Italians, who often forgo treatment due to waiting times and costs. Consequently, new insurance products are being developed to cover medical expenses in cases where the NHS doesn't provide coverage, or where public medical treatment is delayed. The mentioned technologies have been than implemented to insurance contract, refiguring them into parametric contracts. This reconfiguration appears to reinforce datafication, surveillance capitalism, and existing inequalities, particularly to the detriment of patients. This essay analyses InsurTech strategies, focusing on insurance contracts for medical expenses that are driven by data, to assess their feasibility according to Private and data protection laws.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Le tecnologie per il monitoraggio remoto, i dispositivi indossabili, l'IoT e le applicazioni digitali hanno accelerato la trasformazione dell'assistenza sanitaria nel periodo post-pandemico. I modelli di cura proattiva favoriscono la gestione delle patologie fuori dalle strutture ospedaliere e consentono agli individui di controllare e orientare i propri percorsi di salute, migliorando la capacità decisionale. Tuttavia, tali progressi non hanno inciso sulla povertà sanitaria che colpisce milioni di italiani, i quali rinunciano alle cure a causa di tempi d'attesa e costi. Ne conseguono nuovi prodotti assicurativi destinati a coprire spese mediche non coperte dal SSN o soggette a ritardi. Le tecnologie menzionate sono integrate nei contratti assicurativi, riconfigurati in forma parametrica. Questa evoluzione intensifica dataficazione, capitalism della sorveglianza e disuguaglianze, incidendo sui pazienti. Il saggio analizza le strategie InsurTech e la sostenibilità dei contratti sanitari data-driven alla luce del diritto privato e della normativa sulla protezione dei dati.

Keywords: health; health insurance; InsurTech

Summary: 1. Introduction: Health and post-pandemic Healthcare in the Italian context. – 1.1. Medical Poverty. – 1.2. Insurance contracts and new technologies at the rescue. – 2. A taxonomy attempt for AI-driven healthcare and insurance. – 2.1. AI in Healthcare delivery. – 2.2. From clinical IoTs to consumer wearables. – 2.3. From eHealth to InsurTech: when data exit the therapeutic sphere. – 3. Health Insurance. – 4. IoTs and HI. – 4.1. AI-driven contracts implications. – 4.2. The premium narrative. – 5. AI-driven HI and Data Protection. – 6. Conclusion.

1. Introduction: Health and post-pandemic Healthcare in the Italian context.

The Italian Constitution enshrines the right to health as a fundamental guarantee, explicitly recognised in Article 32, which protects individual wellbeing and proclaims the duty of the Republic to safeguard health as both a collective interest and an individual right. This constitutional protection has traditionally been interpreted in two complementary senses.[1] On the one hand, within a positive dimension, it imposes on the public authorities the duty to provide access to healthcare services and to structure a health system that enables people to obtain necessary treatments across the national territory. On the other hand, on a negative declination, it protects individuals against involuntary medical interventions, limiting compulsory treatments to circumstances expressly provided for by law and typically justified only by extraordinary public-health needs.

The right to health, therefore, operates together with the related right of self-determination in healthcare, which recognises patients' decisional autonomy while situating that autonomy within the therapeutic relationship, clinicians, hospital institutions, and patients are expected to cultivate.[2]

[1] On the different meaning of health, see F Minni, A Morrone, 'Il diritto alla salute nella giurisprudenza della Corte costituzionale italiana' (2019) Rivista AIC 3, 9 ff.
[2] S Rodotà, *La vita e le regole* (3rd ed., Feltrinelli 2018); G Alpa, 'Il diritto all'autodeterminazione e le direttive anticipate sulle cure mediche' (2006) Riv. crit. dir. priv. 83; G Alpa, G Resta, *Le persone fisiche e i diritti della personalità* (Utet Giuridica 2005); A Santosuosso, 'Dalla salute pubblica all'autodeterminazione: il percorso

Despite the robust constitutional framing, the reality of accessing healthcare in Italy reveals a persistent tension between formal entitlements and practical availability. In practice, the foundational and absolute nature of the rights invoked collides with structural obstacles that hamper timely access to the National Health Service. Those obstacles, including shortages of personnel, regional disparities in service provision, and, most of all lengthy, waiting times for diagnostic and specialist procedures, effectively dilute the meaningfulness of the constitutional guarantee.

The gap [3] between guaranteed rights and realised access to healthcare produces what may be termed a devaluation of the fundamental right to health, one that has concrete social and economic consequences for individuals and communities. Therefore, only those who have the financial resources to access treatment at private facilities or who have the time to wait for treatment under the public or affiliated system can effectively exercise their right to health.

One of the most worrying consequences is the emergence of a form of "medical poverty". [4] Large segments of the population defer or forgo care because of economic constraints or because public provision is inaccessible in a timely fashion.

Recent official reports indicate that roughly one person in ten renounced visits or treatments in the prior year because of excessive waiting lists, prohibitive costs, or logistical difficulties. Hence, medical poverty affects a large amount of people: a share equivalent of 5.8 million people in 2024, in the Italian context.[5]

1.1. Medical Poverty.

The phenomenon of medical or health poverty in Italy denotes the systematic inability of individuals or households to obtain essential healthcare services, including access to medicines, primary care and diagnostic procedures. The condition is determined by economic, organisational or social barriers, resulting in unmet health needs and increased vulnerability for already vulnerable people affected by diseases. It is a multidimensional form of exclusion in which financial hardship, gaps in service provision and social determinants converge to prevent access to necessary care. It encompasses

---

del diritto alla salute', in M Barni, A Santosuosso (eds.), *Medicina e diritto* (Giuffrè Editore 1995) 95; R Pucella, *Autodeterminazione e responsabilità nella relazione di cura* (Giuffrè Editore 2010) 69; C Castronovo, 'Autodeterminazione e diritto privato' (2010) Eur. dir. priv. 1037; T Pasquino, 'Autodeterminazione', in Aa.Vv., *Le parole del diritto. Studi in onore di Carlo Castronovo* (Jovene 2018) 119; B Salvatore, *Informazione e consenso nella relazione terapeutica* (ESI 2012) 164; G Facci, 'Brevi osservazioni in tema di funzione riparatoria della responsabilità civile e violazione del sanitario del dovere di informazione' (2008) Resp. civ. prev. 408; E Palmerini, 'Il danno patrimoniale da violazione del consenso informato', in E Navarretta (ed.), *Il danno non patrimoniale. Principi, regole e tabelle per la liquidazione* (Giuffrè 2010) 532.

[3] A Luciano, '*Dalle società di mutuo soccorso alla mutualità. Risposte alla crisi del welfare'* (2012) Euricse Working Paper 32, 16.

[4] S Sarti, M Terraneo, M Tognetti Bordogna, 'Poverty and private health expenditures in Italian households during the recent crisis' (2017) 3 Health Policy 307-314; L Pesenti, 'Healthcare Poverty and Access to Healthcare Services in Italy: The Challenge of Public-Third sector Integration' (2025) Riv. trim. Scienza dell'Amministrazione 1-22.

[5] A Petrelli, A Rosano, A Rossi, 'The geography and economics of forgoing medical examinations or therapeutic treatments in Italy during the economic crisis' (2019) Public Health 12.

direct costs, such as out-of-pocket payments for drugs and visits, or indirect costs, such as transport to go in other Italian regions or abroad and even lost earnings, as well as structural barriers, like long waiting lists and regional disparities between structures and personnel, that force people to forgo or delay treatment.

Between the listed factors, the principal drivers of forgone care are long waiting times and economic barriers, with the proportion of the population refraining from care which has increased over the years.

The situation creates a paradox, because the lack of prevention and the postponement of treatment lead to the hospitalisation of cases that become more serious, with the risk of higher costs for the national health service.

Waiting lists[6] themselves are emblematic of systemic strain and regional divergence.[7] Independent health research institutes[8] and national platforms[9] monitoring appointment backlogs report that only about half of scheduled services meet the established maximum waiting times; for the remainder, the situation is critical, with a substantial share of procedures subject to delays measured in months rather than days.

According to CENSIS report,[10] very few patients secure specialist appointments within days of booking, while a non-trivial share face waits more than six months, especially women, foreigners and low-income household members.[11] These delays undermine preventive care, worsen prognoses, and push users towards private alternatives that entail out-of-pocket expenditure.

1.2. Insurance contracts and new technologies at the rescue.

The interaction between financial pressure and service delays fuels the penetration of private expenditure into the healthcare landscape, especially after Covid-19 spread.[12] When public provision fails to deliver timely care,

---

[6] On the matter, it is worth mentioning that the Ministry of Health recently adopted guidelines on waiting lists: D.M. 17 february 2025, *Linee guida della Piattaforma nazionale delle liste di attesa e criteri di interoperabilità con le piattaforme regionali*, available at: <https://www.trovanorme.salute.gov.it/norme/renderNormsanPdf?anno=2025&codLeg=105773&parte=1%20&serie=null>. In literature, E Rogai, 'La crisi delle prenotazioni e delle liste d'attesa nella sanità italiana: situazione attuale e spunti di miglioramento, (2022) 5 Italian Journal of Prevention, Diagnostic and Therapeutic Medicine 17-23.

[7] It is worth mentioning that health is a subject which obeys to the concurrent competence of Regional and State level legislator, according to art. 117 Cost., and this affects the way healthcare is managed and provided on the Italian territory.

[8] Report Osservatorio GIMBE, *La mobilità sanitaria interregionale nel 2018*, Bologna, 2020, 2, available at: <www.gimbe.org/mobilita2018>.

[9] The National Waiting List Platform (PNLA), established by Article 1 of Law No. 107 of 29 July 2024, has recently become available on the AGENAS Transparency Portal. The Platform, created by AGENAS, aims to monitor, on a national scale, waiting times for outpatient services, with particular attention to compliance with the timelines set for the different priority classes. The platform is available at: <https://www.portaletrasparenzaservizisanitari.it/pnla/>.

[10] Fondazione CENSIS, Intesa San Paolo RBM Salute, *IX Rapporto sulla sanità pubblica, privata e intermediata - annualità 2019-2020*, 2021, 74-93.

[11] A Petrelli and others, 'The geography and economics of forgoing medical examinations or therapeutic treatments in Italy during the economic crisis' (2019) Public Health 19, 10 ff.

[12] R Santagata, 'Polizze assicurative parametriche (o index-based) e principio indennitario' (2022) Rivista di Diritto Civile 134-172; S Landini, 'Data sharing and innovation in the insurance industry. First thoughts' (2025) European Journal of Privacy Law and Technologies 12; MC Gaeta, DS D'Aloia, InsurTech in Italy: opportunity, risks and applicable regulation (2021) 2 European Journal of Privacy Law and Technology 10-23; E Battelli, 'Insurtech ed evoluzione dell'offerta di polizze sanitarie: tra innovazione tecnologica e i nuovi

patients and households increasingly turn to private providers or purchase health insurance to secure access to high-cost interventions, faster diagnostics, or continuity of care.[13]

Private medical insurance, therefore, acquires new functions and dimensions, while raises new concerns. First, health insurance (in the following sections, HI) broadens its social security function; second, it becomes both a safety valve, that enables those who can afford it to circumvent public-sector bottlenecks, and a tool, to preserve the substantive enjoyment of the constitutional right to health in practice. Third, the growing relevance of private HI for access to essential and high-cost care thus raises pressing questions about privacy, surveillance capitalism and most of all the risk of stratified access to health services.[14]

Concurrently, the healthcare and insurance spheres are being reshaped by a technological revolution driven by artificial intelligence (in the following parts, AI). AI's incursion into healthcare operates on several fronts.

The first concerns the reconfiguration of healthcare delivery itself: diagnostic algorithms, predictive analytics, automated triage systems, and AI-augmented clinical decision support have the potential to modify workflows, redistribute tasks within clinical teams, and alter the therapeutic relationship between institutions, clinicians, and patients. These innovations promise gains in efficiency, diagnostic accuracy, and personalised treatment pathways. Yet, they also introduce new profiles of risk: as often recalled, these new technologies may affect healthcare with algorithmic bias, opacity in decision-making, liability uncertainties, and threats to patient privacy.

To strike a balance between the two sides of the coin, the European Community first and the European Union later committed to regulate the phenomenon to protect citizens' rights. In fact, it is possible to detect a progressive regulatory layering in eHealth and mHealth,[15] since European

servizi assicurativi in campo medico' (2022) 1 Contratto e impresa 52-91, in particular 52; M Hazan, 'Gli effetti della pandemia sulle polizze di responsabilità sanitaria ma non solo: una riflessione sulle conseguenze per il mercato assicurativo', in R Caminiti, M Frigessi di Rattalma, P Mariotti (eds.), *Gli effetti della pandemia sulla responsabilità sanitaria e sulla sua assicurazione tra norme, giurisprudenza di legittimità et etica* (Maggioli Editore 2021) 73-85. The A. highlights how impactful is this new insurtech approach in Italy, as a new pillar that stands alone and counterparts the public national and regional sector. On the matter, see also B Nayak, SS Batthacharyya, 'The Changing Narrative in the Health Insurance Industry: Wearables Technology in Health Insurance Products and Services for the COVID-19 World' (2021) 4 Journal of Medical Management 550-558.

[13] It is possible to confirm this affirmation in the data gathered by Accenture in 2020, available at: <www.iotiassicuro.it>.

[14] S Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75-89; C Gidaris, 'Surveillance Capitalism, Datafication and Unwaged Labour: The Rise of Wearable Fitness Devices and Interactive Life Insurance' (2019) 17 Surveillance and Society 132-138; K De Blasio, 'Il marketing algoritmico tra tutela della privacy e pratiche commerciali scorrette' (2025) 3 Riv. it. Informazione e informatica 379 ff.

[15] For the different notion of eHealth and mHealth, see T Mulder, 'The impact of the European Medical Device Regulations on the development and use of mhealth apps in Europe', in J Madir (ed.), *HealthTech: Law and Regulation* (Edwar Elgar Publishing 2020) 329-353; I Rapisarda, 'La privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche' (2023) *Nuove Leggi Civili Comm* 184-213. On telemedicine, see M Faccioli, 'La responsabilità sanitaria in telemedicina' (2021) 3 Resp. civ. prev. 740 ff.; RY Cheng, B Robin, 'Telemedicine: Opportunities and Challenges – A US Perspective', in J. Madir (ed.), *HealthTech: Law and Regulation* (Edwar Elgar Publishing 2020) 354-373. The "telemedicine" concept emerged in the 1960s due to the need for medical services in space for the National Aeronautics and Space Administration (NASA) and the military. While "telehealth", which is often used as a synonim, refers to a broader application of devices and services for health and self-health without clinicians and medical services involved: more information

instruments sought to capture rapidly evolving technologies and uses. Foundational device directives such as the Active Implantable Medical Devices Directive 90/385/EEC, the Medical Devices Directive 93/42/EEC and the In Vitro Diagnostic Directive 98/79/EC established early safety, conformity and market access principles for implants, general medical devices and diagnostics, respectively. Later, Regulation 2017/745/EU for medical devices and Regulation 2017/746/EU for in vitro diagnostics were adopted and, in parallel, data protection developed along a distinct but intersecting path, with the Data Protection Directive 95/46/EC and the General Data Protection Regulation 2016/679/EU.[16] Recently, new European initiatives,[17] such as the European Health Data Space Regulation (in the following paragraphs, EHDS), aim at enabling cross-border health data exchange and interoperability with MyHealth@EU infrastructure and related policy instruments. Moreover, the sector is impacted by Digital Services Act,[18] Digital Markets Act,[19] Data Governance Act,[20] Data Act,[21] and AI Act.[22]

The second front, which will be the principal focus of this paper, is the reconfiguration of HI policies. AI-enabled tools and the clinical and consumer-level Internet of Things (IoTs), including wearable devices, allow real-time monitoring of health metrics.[23] These devices allow the generation of highly granular risk profiles and better and broader insurance coverage. In the US,[24]

---

are provided by NASA, A Brief History of NASA's Contributions to Telemedicine, 2013, <https://www.nasa.gov/wp-content/uploads/2024/03/nasatelemedicine-briefhistory.pdf>; WHO, *Telemedicine – Opportunities and Developments in Member States,* 2010, <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.afro.who.int/publications/telemedicine-opportunities-and-developments-member-state&ved=2ahUKEwi039PLjJKRAxV3xQIHHQfXFOkQFnoECBsQAQ&usg=AOvVaw3pjxr8V-3NszsEgJFyc-ni>; E Giusti, 'La sanità elettronica: dati personali relativi alla salute, applicazioni e rischi (e-Health: personal health data, applications and risks)' (2023) Riv. it. Med. legale 85 ff.

[16] Persistent tensions remain where regulatory scopes diverge. For example, consumer wearables may fall outside medical device classification while the personal data they produce nonetheless qualify as health data under the GDPR. Such mismatches underscore the continuing need for interpretative guidance, coordinated enforcement and adaptive governance to ensure coherent protection, innovation and patient safety across overlapping legal regimes.

[17] A Morace Pinelli (ed.), *Dalla Data Protection alla Data Governance: il Regolamento (UE) 2022/868,* (Pacini Giuridica 2024); id., Data Act. Introduzione interdisciplinare e commentario al regolamento (UE) 2023/2854, (Pacini Giuridica 2025); id., la circolazione dei dati personali: persona, contratto e mercato (Pacini Giuridica 2022).

[18] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Official Journal L 277, 27 october 2022).

[19] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Official Journal L 265, 12 october 2022).

[20] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Official Journal L 152, 03 june 2022).

[21] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Official Journal L, 22 december 2023).

[22] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Official Journal L, 12 july 2024). It is worth mentioning that, on the matter, Italy adopted the first regulation on AI applications in Europe: law 23 September 2025, no. 132, which provides *Disposizioni e deleghe al Governo in materia di intelligenza artificiale* (Provisions and delegations to the Government on artificial intelligence), published G.U. 25 September 2025, no. 223, which recently entered into force, on 10 October 2025.

[23] P Poletti, 'Data Act ed equa condivisione dei dati generati dagli apparati IoT: di quali dati si tratta?', in A. Morace Pinelli (ed.), *Data Act*, 153-174.

[24] A Troiano, 'Wearables and Personal Health Data: Putting a Premium on Your Privacy' (2017) Brooklin Law Review 1715-1753; M Antona, C Stephanidis (eds.), *Universal Access in Human-Computer Interaction. Access*

India,[25] China,[26] Japan,[27] and Germany,[28] insurer policymakers are already experimenting with data-driven underwriting,[29] personalised premiums, and contract terms conditioned by the use of sensors and telemonitoring devices, to promote a better policy-holder profiling.[30] This shift[31] is affecting or making its way even in Italy as well,[32] and raises crucial questions about how AI-driven technologies influence individual choices regarding care-seeking, how contractual coverage mediates access to services, and how the diffusion of such technologies may mitigate or exacerbate existing inequalities in healthcare access.

This essay therefore undertakes a taxonomy of AI-driven evolutions in healthcare and insurance markets, in order to examine how AI influences patient/consumer/insured behaviors, and at the same time how insurance contracts are reconfigured whenever they are driven by data gathered through IoTs and wearables, as well as whether these contractual forms are lawful and protective of policyholders' rights. Special attention will be given to data protection frameworks, notably the GDPR and following legislations, and to sector-specific initiatives like the 2025 EHDS Regulation, assessing the compatibility of conditional insurance models with privacy and non-discrimination.

After laying out technological and market developments, the paper will move to a legal assessment of HI that factor in continuous monitoring (and profiling), behavioral incentives, and most of all algorithmic underwriting. The analysis will assess the level of user protection, interrogating whether existing regulatory instruments adequately address asymmetries of information, algorithmic opacity, and the potential for indirect exclusion from coverage. The ultimate objective is to delineate pathways by which innovation can be harnessed to enhance access to care while safeguarding the constitutional

---

to Learning, Health and Well-Being (Springer 2015) 288-299; ME Maccarini, *L'assicurazione sanitaria negli Stati Uniti d'America* (Consorzio Pavese per gli Studi postuniversitari 1994).

[25] P Kaur, M Singh, 'Exploring the impact of InsurTech adoption in Indian life insurance industry: a customer satisfaction perspective' (2025) 2 TQM Journal 457-483.

[26] S Cao, H Lyu, X Xu, 'InsurTech development: Evidence from Chinese media reports' (2020) Technological Forecasting and Social Change, 161.

[27] Y Luen Ma, Y Ren, 'InsurTech. Promise, threat or hype? Insights from stock market reaction to InsurTech innovation' (2023) Pacific-Basin Finance Journal 80 <https://doi.org/10.1016/j.pacfin.2023.102059>.

[28] T Oletzky, 'InsurTech in the United States and Germany – What are the Drivers behind the Different Business Models' (2023) 26 Risk Management and Insurance Review 485-511.

[29] A Spender and others, 'Wearables and the internet of things: considerations for the life and health insurance industry' (2019) 24 British Actuarial Journal 1-31; D Neumann, V Tiberius, F Biendarra, 'Adopting wearables to customize health insurance contributions: a ranking-type Delphi' (2022) Medical Informatics and Decision Making 22, 112.

[30] On profiling, see A Spangaro, 'Il concetto di profilazione tra "direttiva madre" e GDPR' (2022) Giur. it. 1579-1587; O Sesso Sarti, 'Profilazione e trattamento dei dati personali', in L Califano - C Colapietro (eds.), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679* (ESI 2017) 573-626.

[31] I Cimbru, J Wagner, AZ Röschmann, 'On IoT-enabled risk prevention and insurance: A systematic literature review' (2025) Risk Management and Insurance Review 1-52.

[32] On the matter, see the analysis provided by ANIA, The Italian insurance market and new investment trends under Solvency II, 2017, available at: <https://www.ania.it/documents/35135/126704/Italian-Insurance-in-figures-2017.pdf/684a880f-8919-83d2-7f11-503dfea85f16?version=1.0&t=1575555161527>; also see FinTech & InsurTech Observatory of the School of Management of the Politecnico di Milano, 'Cresce il Fintech in Italia: quali sono le startup e i numeri e della rivoluzione', 15 December 2021 available at: <https://blog.osservatori.net/it_it/FinTech-in-italia>.

right to health and the autonomy of patients, thereby preventing a deepening of medical poverty through technological and market distortions.

2. A taxonomy attempt for AI-driven healthcare and insurance.

The application of robotic and artificial intelligence to medicine has become a pervasive and recurrent theme in the scientific literature, even within Italian scholarship, where debates increasingly mirror international conversations. As habitually stressed by existing literature,[33] the new technologies allow faster, and more accurate diagnostic processes intended to prevent disease progression, reduce hospital admissions, particularly among patients with chronic conditions.

It is worth mentioning, that many of the innovations ascribed to AI in medicine are already tangible rather than merely speculative. The problem is that to achieve these goals of evolution by innovation a vast set of data is required, as well as its proper management and compatibility with the rights guaranteed by supranational and internal sources. Furthermore, these technologies are not yet within everyone's reach. Differently, autonomous tracking mechanisms, by consumer-level IoTs or wearables, are within the reach of everyone or, at least, a large amount of people worldwide.[34]

2.1. AI in Healthcare delivery.

Artificial Intelligence is to be understood as the branch of computer science and engineering that imitates human cognitive functions by means of algorithms, employing sequences of elementary instructions in the form of lines of code to create artefacts that exhibit behaviour commonly regarded as intelligent. These systems are software, that could be embedded in hardware: when these systems are tasked with a complex objective, they acquire data and provide their interpretation, by reasoning on prior knowledge and processing information derived from those data, later they select the best action to achieve the specified goal. AI systems may operate using symbolic rules or by learning numerical models and adapting behaviour by analysing how the environment has been affected by prior actions.

---

[33] G Comandé, 'Tecnologie e metamorfosi del danno e della responsabilità sanitaria' (2024) 2 Danno resp. 153-160; F Cerea, 'Intelligenza artificiale al servizio dei pazienti per il contrasto a CoVid-19' (2020) 3 Nuova Giur. Civ. Comm. 45-49.

[34] According to recent studies, IoT spread is likely to reach 31 billion installed units by 2025, each equipped with sensors collecting data from a vast array of physical objects, such as automobiles. On the matter, see M. Hung (ed.), *Leading the IoT. Gartner Insights on How to Lead in a Connected World*, available at <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf>. This great availability of IoT and wearable has an immediate consequence: as technology costs decrease, the market share of tech-based firms increases, leading to a shift in market structure where low-risk individuals are more likely to select tech insurers. On the matter, see M Soleymanian, CB Weinberg, T Zhu, 'Insurtech, sensor data, and changes in customers' coverage choices: Evidence from usage-based automobile insurance' (2025) 92 Journal of Risk and Assurance 227-256.

Among the many learning techniques that populate the broad field of AI, two are particularly salient for this analysis: Machine Learning (in the following parts, ML)[35] and Deep Learning (in the following parts, DL).[36]

ML denotes a set of methods whereby computer systems improve performance on tasks by identifying patterns in data and making predictions or decisions without being explicitly programmed for each instance. These models typically require feature engineering and can be trained with comparatively modest datasets, and they often permit greater interpretability of decision logic.

Differently, DL is a subset of ML, that utilises multilayered artificial neural networks to learn hierarchical representations of data. It is defined as deep, since it has multiple processing layers, enabling the automatic extraction of complex features from large volumes of data and supporting supervised, semi-supervised or unsupervised training regimes.

The medical sector[37] is among the most permeated by intelligent systems, a phenomenon driven by the digitalisation of imaging diagnostics, the adoption of digital reporting systems supplanting paper records, advances in molecular biology technologies and the proliferation of Internet of Things devices that continuously generate clinical and physiological data. In practice, AI in medicine spans a range of applications: automated image analysis for radiology and pathology that assists detection, segmentation and classification of lesions; predictive analytics for patient risk stratification and prognosis; natural language processing tools that extract structured information from clinical notes and generate draft reports; personalised medicine platforms that integrate genomic, proteomic and clinical data to suggest tailored therapies; remote monitoring and decision support enabled by wearable sensors and IoT devices; and robotic systems that augment surgical precision or automate routine laboratory workflows.

As described in the examples, the use of artificial intelligence in medicine is heterogeneous in its applications. To exemplify the applications, it has been noted that AI can function as an integrative adjunct to clinical teams or as a substitute for tasks performed by doctors and hospital staff.[38]

In substitutive applications, AI may carry out, wholly or partly, the actions identified as necessary for a patient's condition, yet this does not remove the clinician's and the institution's duty of care and supervisory responsibility, since physicians and healthcare organisations remain legally accountable for overseeing the AI's performance and intervening when outputs are inappropriate or uncertain. For example, AI may perform diagnostics, which will be assessed by the personnel to address the appropriate therapeutic path

[35] The Royal Society, 'Machine learning: the power and promise of computers that learn by example' (2017) 15.

[36] F Cerea, 'Intelligenza artificiale al servizio dei pazienti per il contrasto a CoViD-19' (2020) Nuova Giur. Civ. Comm 47.

[37] For detailed analysis of the application of AI in medicine, see U Ruffolo, 'Le "mobili frontiere" della responsabilità medica' (2021) 2 Giur. It. 456-516; Comandé (n 33) 156 ff.; G Votano, 'Intelligenza artificiale in ambito sanitario: il problema della responsabilità civile' (2022) 6 Danno resp. 669-679, in particular 670-671; O Venier, 'Intelligenza Artificiale, Blockchain e mondo IoT: l'esperienza degli operatori' (2020) 2 Dir. Industrale 166-171; E Verona, 'Errore diagnostico e intelligenza artificiale: profili di responsabilità nell'imaging medico' (2025) 4 Nuova Giur. Civ. Comm. 1075-1084.

[38] Comandé (n 33) 158 ff.

or alternatively AI may suggest how to treat the patient for the diagnosed pathology.[39]

In integrative roles AI supports clinicians and personnel by enhancing diagnostic accuracy with Clinicians Decision Support Systems (CDSS), stratifying risk, offering decision aids, suggesting relevant clinical guidelines[40] and flagging exceptional factors that fall outside guideline-designated cases, thereby augmenting rather than replacing human judgement.

2.2. From clinical IoTs to consumer wearables.

IoT in healthcare gather a network of connected devices and sensors that collect, transmit and sometimes process data across local or internet-based networks to support monitoring, automation and analytics.[41] This category is quite broad and spans environmental sensors, bedside monitors, infusion pumps and implantable devices. [42] These devices are characterized by connectivity and the capacity to feed continuous or periodic data into centralised platforms or distributed analytic engines.[43]

The integration of AI with IoT ecosystems is set to support continuous care in and most of all outside hospital walls, allowing earlier detection of deterioration and more confident early discharge strategies. This outcome has been stressed even by the World Health Organization (WHO): eHealth and mHealth applications can help the EU Member States ensure that «national health systems meet the demand for the delivery of high quality, readily available services in spite of zero-growth or decreasing health budgets».[44]

Wearables are a subset of IoT devices designed to be worn on the body or incorporated into jewellery, clothing, sunglasses, sensors, and other kind of accessories. They capture physiological or behavioural signals, namely heart rate, movement, sleep, glucose levels or respiratory metrics, either continuously or intermittently. These devices can provide immediate feedback to the wearer or stream data for clinical review or to other parties.

---

[39] A Fiorentini, 'Machine Learning e dispositivi medici: riflessioni in materia di responsabilità civile' (2021) 10 Corr. Giur. 1258-1268.

[40] M Faccioli, 'Intelligenza sanitaria e responsabilità sanitaria' (2023) 3 Nuova Giur. Civ. Comm. 732-743; AG Grasso, 'Diagnosi algoritmica errata e responsabilità medica' (2023) 2 Riv. dir. civ. 334-360.

[41] O Venier, 'Intelligenza Artificiale, Blockchain e mondo IoT', 167. On IoT, see also V Zeno Zencovich, 'Ten Legal Perspectives on the "Big Data" Revolution' (2016) Concorrenza e Mercato 29 ff.

[42] M Ferrari, 'Il rischio putativo e le nuove frontiere "assicurative" degli ecosistemi digitali' (2024) 2 Danno resp. 181-187, in particular 185-186.

[43] On wearables, see E Germani, L Ferola, 'Il wearable computing e gli orizzonti futuri della privacy' (2024) Diritto dell'Informazione e dell'Informatica, 75 ff.

[44] WHO Europe, Health Topics, Health Systems, E-Health, 2019, available at: <http://www.euro.who.int/en/health-topics/Health-systems/e-health/e-health-readmore>. On the matter, see European Commission, Final report – Benchmarking Deployment of eHealth among. General Practitioners, Brussel, 2013, available at <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4897>; id., Green paper on mobile health, Brussel, 2014, available at <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=518>. The literature on the matter is already vast: for an overview, see G Eysenbach, 'What is eHealth?' (2001) 2 Journal Med. Internet Res. 20 ff.; id., EHEALTH: Improving and Standardizing Evaluation Reports of Web-based and Mobile Health Interventions, (2011) 4 Journal Med. Internet Res. 126 ff.; id., 'Towards ethical guidelines for e-health: JMIR Theme Issue on eHealth Ethics' (2000) Journal Med. Internet Res. 7 ff.; T Mulder, The impact of the European Medical Device Regulations on the development and use of mhealth apps in Europe 330.

As stated for other AI applications, IoT devices and wearables enable earlier detection of deterioration, more precise therapies, and improved self-management by sane, sick and chronic patients.[45] For healthy individuals, consumer-grade fitness trackers and smartwatches monitor activity, sleep and resting heart rate, providing behavioural feedback that supports primary prevention and healthier lifestyles. In acutely ill patients, hospital-grade IoT sensors and connected monitoring systems stream real-time vital signs into early-warning algorithms that can detect deterioration ahead of routine nursing observations, prompting rapid clinical review. For patients with chronic conditions, the impact is especially pronounced.[46]

2.3. From eHealth to InsurTech: when data exit the therapeutic sphere.

The value of the above-mentioned different devices and, above all, the data they collect is not only appreciated in the medical field, to facilitate or speed up the provision of healthcare services or, broadly speaking, administrative services carried out in a public or private hospital. Instead, devices and data enable a wide range of value-adding services and benefits to users, consumers and after all policyholders, before entering a healthcare facility. Mobile apps and wearables allow users and consumers to track their biometric data on a day-to-day basis, with smartwatches,[47] smart fridges, mirrors, scales. There is no doctor supervising the collection and processing of this data: the data is collected because the person wants to know how many steps they have taken or their water or vitamins intake, what their body mass index is, what their eating habits are, what their stress level is, their cycle and their fertility peaks, their exercise rhythm and intensity, their physical improvements, and so on.

Consumers' willingness to collect data through these devices and software can enable physician to understand better the patient condition but it can as well serve other functions such as economic exploitation. The possibility of exploiting this data economically paves the way for new contractual arrangements. Thus, we move from reactive to proactive negotiation, from customership to membership, from a transactional to a more social view of the contract, from an approximation of the contractor's condition to a tailor-made contractual solution for the individual, and from analogue and local negotiation to digital and, at the same time, global negotiation that transcends territorial boundaries.[48]

The potential described above is also valued in contracts covering medical expenses: a field now referred with the neologism InsurTech.[49] InsurTech is an

[45] P Thottempudi, R Madhavi Konduru, H Bindu Valiveti, S Kuraparthi, V Kumar, 'Digital health resilience: IoT solutions in pandemic response and future healthcare scenarios' (2025) 6 Discover Sustainability 144.
[46] B Keller, *Big Data and Insurance: Implications for Innovation, Competition and Privacy,* Geneva Association - International Association for the Study of Insurance Economics (2018) 3.
[47] K De Blasio, 'Il marketing algoritmico tra tutela della privacy e pratiche commerciali scorrette', 379 ff.
[48] S Møllegaard, 'Six Mega-trends that will take Insurance back to the Future', in SLB Vanderlinden and others (eds.), *The InsurTech Book. The insurance Technology handbook for Investors, Entrepreneurs and Fintech Visionaries* (Wiley 2018) 57-60.
[49] V Ricciardi, 'InsurTech Definition as its Own Manifesto', in S Christi, J Barberis (eds.*), The InsurTech Book: The Insurance Technology Handbook* 6-8; S Cruz Rambaud, J Lopez, 'Insurtech, Proptech, and Fintech Environment: Sustainability, Global Trends and Opportunities' (2023) 15(12) Sustainability 9574; A Gramegna, P Giudici, 'Why to buy insurance? An explainable artificial intelligence approach' (2020) 8(4) Risks 137; A Vigil Iduate, 'InsurTech' (2019) 53 Rev. Ibero-Latinoam. Seguros 173-180; Ö Gürses, 'Insurance Law

ecosystem,[50] comprehensive of a series of contracts and services, which are either stipulated as an addendum to an employment contract or stipulated directly by the person who intends to better allocate healthcare costs. These solutions are innovating the market and have already received the attention of many international studies. These contracts integrate innovation, technologies and automation into contracts, following the principle of "digital by default".

The phenomenon addresses specifically insurance policies to better frame the risk pool, to provide more coverage and transparency, to optimize value creation, to improve customer experience by adopting a user-centric approach and to overcome the insurance market systemic failure.[51] The contract is established between a policymaker and a policyholder: the latter is a consumer and the weaker party in the relationship, in a particularly vulnerable position because they are or will soon be a patient undergoing medical treatment. Therefore, person's data (a consumer's data and then a patient's data) are used to draw up a B2C contract; consequently, their behaviour, in the therapeutic context, will also be shaped or at least influenced.

As it is possible to understand from the premise, there are several benefits, but there are also multiple risks and most of all areas of interest for scholars who are attentive to these different contractual configurations, if not hybridisations. This is why it is essential to first understand the nature, purpose, structure and function of health insurance contracts and then assess how these policies are changing, or even evolving, within the phenomenon of Insurance of Things (INSoT) in InsurTech.

3. Health Insurance.

Health insurance (HI) evolved into novel,[52] usage-based, contractual schemes that aim at transferring[53] the costs connected to the risks depending on future pathological conditions and any other connected conditions of the insured person.

---

and AI. Demystifing InsurTech', in E. Lim, P. Morgan (eds.), *Private Law and Artificial Intelligence* (Cambridge University Press 2024) 534-556. According to these Aa., the neologism InsurTech is used to frame the application of AI methods to (big) data retrieved from users' engagement via smartphones or other media, in order to close the gap between non-life insurance providers and consumers, thereby improving the protection provided and better allocate overheads, which are quite high in this sector, as premiums for insured well-behaved customers. In the Italian literature, on the matter, see Battelli (n 12) 59-91; A Luberti, C Tabarrini, 'Insurtech. Una ricognizione empirica e giuridica' (2018) Consumers' Forum. Il cittadino nell'era dell'algoritmo 93 ff.; D Porrini, 'Big Data, personalizzazione delle polizze ed effetti nel mercato assicurativo', in V Falce, G Ghidini, G Olivieri (eds.) *Informazione e big data tra innovazione e concorrenza* (Giuffrè 2018) 319 ff.; MC Gaeta, DS D'Aloia, 'InsurTech in Italy: opportunity, risks and applicable regulation' (2021) 2 European Journal of Privacy Law and Technology 10-23.

[50] V Ricciardi (n 49) 6.

[51] S Tunstall, 'Why is Insurance Failing?', in SLB Vanderlinden, SM Millie, N Anderson, S Chishti (eds.) *The InsurTech Book* 9-12.

[52] On the matter, see F Schiavon, *Le spese per cure mediche nella legislazione fiscale e nella riforma sanitaria. Deducibilità Irpef e successioni; Assicurazione privata malattie; Cure all'estero; L'Assistenza pubblica: prestazioni ed oneri contributivi; Normativa fiscale dei prodotti farmaceutici* (Roma 1982) 44-54.

[53] On the transfer technique, see Landini (n 12) 2 ff.; I Partenza, RV Nucci, *L'assicurazione della responsabilità sanitaria. Professionisti e strutture sanitarie, rischi assicurati, profili giurisprudenziali, ipotesi di riforma* (Pacini Giuridica 2022) 19. In the Italian case law, Cass. Civ., Sez. Un., 22 may 2018, no. 12564, in Foro it., 2018, 6, 1900 ff.

The risks are allocated whenever they are not due to violent external causes and the contract does not cover for permanent disability.

Although in the Italian legal system the right to health is a fundamental and absolute right, which gives rise to the possibility of access to free healthcare for the poor, art. 38 Cost. allows for the supplementary fulfilment of the social security function and to supplement the social rights of individuals through the exercise of negotiating autonomy.[54]

These pacts tend to challenge and drift from traditional insurance dichotomy, which is usually based – at least in Italy, under art. 1882 c.c. and reflected on art. 38 of IVASS Regulation – on the main difference between the types of risks covered, considering the so-called damages branch and life branch.[55] While accident insurance, which qualifies as part of the damages' insurance branch , usually includes insurance for healthcare costs, the reverse cannot be said to be true. HI covers for the losses which impact on the patient's patrimony[56] and not (or at least, not exclusively) for the body integrity.[57] However, the loss for the patrimony is linked to the body integrity infringement, so this makes HI part of the non-life damages-branch.[58]

HI may cover individual risk or that of family and non-family groups. These contracts recall the instruments for integrative[59] supplementary[60] coverage connected to the work contract and from payment protection insurance,[61] and on a certain level the issues that will be considered for private law insurance pacts could be extended to integrative coverage as well.

HI pacts bind an insurer (the policymaker) and the insured (the policyholder), and these contracts are designed specifically for medical expenses coverage or second medical opinion[62] or hospital stays[63] or recovery periods or even direct access to the health facilities to have access to benefit from a medical treatment, which has a previous pact with the insurance (indirect reimbursement).[64] The direct reimbursement may be complete or may integrate the difference with the national social healthcare assistance. So, HI typically perform a health-security function by reimbursing medical expenses and such reimbursements (or direct payment to the medical facility) may

[54] S Pardini, 'L'assicurazione contro i danni alla persona: sulla vita e sulla salute' in M. Gorgoni, F. Greco (eds.) *Diritto delle Assicurazioni* 320-321.
[55] TV Russo, 'Vigilanza sulle imprese di assicurazione e riassicurazione' in M Gorgoni, F Greco (eds.) *Diritto delle Assicurazioni* 65-92.
[56] G Iorio, 'L'assicurazione del patrimonio e di cose' in M Gorgoni, F Greco (eds.) *Diritto delle Assicurazioni* 337-353; Pardini (n 54) 330.
[57] On the *summa divisio*, see G Fanelli,' La "summa divisio" delle assicurazioni private: riflessioni su un vecchio problema' (1962) 4 Foro it. 51 ff.; Pardini (n 54) 319-335, in particular 330. On the difference, see S Landini, 'Polizze sanitarie nelle dinamiche contemporanee della longevità' (2019) Riv. it. Med. Leg, 2, 511 ff.; Schiavon (n 52) 46.
[58] Partenza, Nucci (n 53) 18 ff.
[59] E Piras, 'Fondi sanitari integrativi e società di mutuo soccorso: le nuove frontiere della sanità integrativa' (2016) Resp. Civ. Prev. 1870 ff.; id. (ed.), *Le attuali prospettive della previdenza complementare e della sanità integrativa* (ESI 2022) 69. These pacts are regulated by l. 23 ottobre 1992, n. 421, which was implemented with d.lgs. 30 dicembre 1992, n. 502.
[60] M Lippi Bruni, S Rago, C Ugolini, *Il ruolo delle mutue sanitarie interattive* (Il Mulino 2012); G Rocco, 'Sanità integrativa: ruolo centrale nel welfare aziendale' (2018) Dir. prat. lav. 1048.
[61] Battelli (n 12) 80 ff.
[62] Landini (n 57) 511 ff.
[63] Schiavon (n 52) 47.
[64] Battelli (n 12) 52.

respond as a reaction or mitigation measure to an acute, newly occurring illness or to ongoing needs arising in daily life, for example the chronic care requirements of an elderly person.[65]

Usually, this contract allows for reimbursement considering the insured risks, however they pose maximum limits and deductibles.

This type of contract can also be entered into to overcome the limitations of national healthcare systems, with international insurance contracts, and/or to guarantee access to treatments that comply with a broader concept of health, understood as a condition of general psychological and physical well-being,[66] aimed at including cosmetic surgery, treatments for physical defects or pre-existing conditions, dental expenses, home care for the elderly and people with disabilities, and nutritional consultations.

These non-life damage-branch insurance policies are aleatory contracts,[67] subject to the principle of indemnity,[68] therefore determining reimbursement of the amount equal to the damage suffered, without determining enrichment to the benefit of the injured party, despite the existence of risk. Therefore, there is no speculative function of risk. Furthermore, they are subject to the rescue obligation, which encourages the insured to prevent and mitigate risk, and to the rule of no-coverage for intentionally caused risks and damages: for example, the HI doesn't provide any coverage for damages and costs related to alcohol, narcotics, psychotropic medication abuse.

HI are offered under private law, structured as premium-paying arrangements in which the premium and the scope of benefits are dynamically linked to individual behaviour and physiological indicators.[69] The insurer is usually tasked with identifying the risk profile of the person seeking cover. To do this, it is necessary to mitigate the information gap and gather data about the individual and their habits. Underwriters use demographic and statistical data,[70] personal questionnaires and the applicant's available clinical records: these factors allow the 'fixed active component' defined ex ante and statically for the insurance premium to be determined.[71] Once the risk picture is assembled, the insurer allocates a risk category and proposes insurance cover. At this point the element of alea becomes clear: the policyholders may behave responsibly, or their condition may deteriorate, or fall ill, or even adopt unhealthy habits or present a condition different from that detected in the pre-

[65] Landini (n 57) 521.

[66] See the new notion in the Preamble at the Constitution of the WHO, as adopted by the International Conference of Health, New York, 19-22 june 1946, available at: <https://apps.who.int/gb/bd/pdf/bd47/en/constitution-en.pdf>. On the matter, see N Vettori, 'Il diritto alla salute alla fine della vita: obblighi e responsabilità dell'amministrazione sanitaria' (2016) Riv. it. med. leg. 1463 ff.; A Guarnieri, 'Profili giuridici della fine della vita umana' (2009) Resp. civ. 1707 ff.; V Rotondo, *Responsabilità medica e autodeterminazione della persona* (ESI 2020) 31 ff.

[67] On the different scholarly opinions on the risk-based nature of the contract, see Partenza, Nucci (n 53) 21.

[68] On the function of the contract, see F Bosetti, *La causa del contratto,* in M Gorgoni, F Greco (eds.) *Diritto delle Assicurazioni* 173 ff.

[69] A Troiano, 'Wearables and Personal Health Data: Putting a Premium on Your Privacy' (2017) Brooklin Law Review 1715-1753; Cimbru, Wagner, Röschmann (n 31) 13-14.

[70] The use of statistics for insurance and risk pooling has been regulated under the Solvency II Directive: Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance.

[71] P Manes, 'Credit scoring assicurativo, machine learning e profilo di rischio: nuove prospettive' (2021) 2 Contratto e Impresa 469-489, in particular 474.

contractual phase. The insurer therefore prices[72] and structures the policy to reflect that uncertainty, often applying exclusions, waiting periods or premium adjustments. This makes these pacts, as other insurance schemes, "contract(s) upon chance":[73] an effective risk assessment needs to manage unpredictable future health developments.

The nature and object of the contract in question also determine its duration,[74] which may depend on a fixed end date or on exposure to risk. In contracts based on a static risk assessment, the contract duration is usually one year, with the possibility of activating the clause that provides for the continuation of the contractual relationship for another year.

Since the HI design is explicitly user-centric,[75] the new trend (or quest) for policymakers is to base the risk analysis on the continuous profiling of the policyholder via IoTs devices and wearables enable far more granular identification of risk, widening the pool of potential customers by matching bespoke offers to heterogeneous risk profiles. These technologies may be developed and integrated in their systems by the insurance policymakers, or they could resort to externalization and partner with tech companies to gather data.[76] These peculiar new dynamic features make these contract known as open insurances[77] and recalls the legal institution already known to the Italian legal system of the so-called estimated policy, as regulated under art. 1908 co. 2 c.c.[78]

Moreover, a distinctive legal and operational feature of many HI products is their embodiment as computable or computational contract, [79] which are generally referred to as "smart contracts".[80] The locution is comprehensive not so much of actual contracts, but consists in contractual terms encoded in a software, which follows a programmable logic, according to which automatically activates, suspends or modifies contractual effects when specified conditions are met. Moreover, streams of biometric and behavioural data feed machine learning models that continuously recalibrate the contract's parameters, producing real-time adjustments to coverage, premiums or benefits. This automation yields efficiency and actuarial refinement, but it also relocates essential decisions from human agents to algorithmic processes whose internal functioning is often opaque to the insured.

---

[72] It is worh mentioning that Big data already impacted on negotiations by allowing the application of personalized prices of which consumers are not aware of, using "group pricing" or "geoblocking" but also "first degree discrimination" considering the single consumer data gathered. On the matter, see M Maggiolino, 'Big data e prezzi personalizzati' (2016) Concorrenza e mercato, 95 ff. On Big data, see V Zeno Zencovich, 'Ten Legal Perspectives on the "Big Data" Revolution' (2016) Concorrenza e Mercato, 29 ff.

[73] This expression as been used in anglosaxon case law: Seaman v Fonereau (1742) 2 Str. 1183, 93 E.R. 1115; Carter v Boehm (1766) 3 Burr. 1905.

[74] M Chironi, 'L'accordo, la forma e la durata del contratto', in M Gorgoni, F Greco (eds.), *Diritto delle Assicurazioni. Attività, Contratti, Responsabilità e Mercato* (Pacini Giuridica 2024) 137.

[75] Battelli (n 12) 52 ff.

[76] Gürses (n 49) 535.

[77] Landini (n 12) 8 ff.; A Camedda, 'La rivoluzione tecnologica nel settore assicurativo: l'avvento dei big data (Big Data & insurance: potential benefits and issues)' (2016) RTDE, 4, 5 ff.; Keller (n 46) 10.

[78] On the estimated policy and its compatibility with the principle of indemnity, see Pardini (n 54) 331.

[79] C Scognamiglio, 'Lo smart contract in ambito bancario', in M. Proto (ed.), *Intelligenza artificiale e rapporti bancari* (Pacini Giuridica 2024) 29-40.

[80] U Salanitro, 'Smart contract tra accordo e rapporto patrimoniale giuridico' (2025) 2 Pactum 141-146; E Battelli, 'Le nuove frontiere dell'automatizzazione contrattuale tra codici algoritmici e big data: gli smart contract in ambito assicurativo, bancario e finanziario' (2020) 4 Giust. civ. 681 ff.; Santagata (n 12) 156.

The heavy reliance on profiling and adaptive algorithms impacts on autonomy considering several levels. The monitoring is relevant so the user can impact in a positive and negative way on the outcomes.

Since the monitoring is so relevant, one must consider that the insured frequently lacks meaningful understanding of which factors will influence the contractual balance, or how the machine learning system synthesises these signals into risk scores and consequent contractual effects.

As considered, monitoring and algorithmic processing constitutes a precondition for concluding the analysed insurance contract, for this reason the policymakers may be compromised in their agency: consent (to contract and data protection first, and to medical treatment later) risks being formal rather than real, and contractual agreement may reflect a disturbed policyholders' determination insofar as they cannot foresee or evaluate the probabilistic and adaptive consequences of their data being continuously processed.

4. IoTs and HI.

In contexts of poverty, where time and money are scarce and public healthcare services are patchy, the deployment of IoT devices and wearable technologies is often presented as a promising and apparently practical solution. Such technologies can be framed as low friction means to encourage healthier lifestyles, to monitor early signs of disease progression and to maintain surveillance of chronic conditions to avoid costly and disruptive hospital admissions.

For populations who cannot afford frequent medical treatments or who are constrained by work and territorial barriers, the idea that a low-cost wearable or a remotely managed sensor network might substitute for parts of face-to-face care has considerable intuitive appeal. The literature and industry discourse increasingly depict IoT and wearables as instruments that extend the reach of health services into daily life, allowing preventive interventions and earlier, less invasive treatments to be delivered at scale. They are, but to a certain extent.

Across healthcare systems, both private and public, these technological affordances have catalysed new models of interaction between patients, clinicians and hospitals, especially where health is not a universal right (i.e. United States). In fact, wearables that measure activity, heart rate, glucose or respiratory parameters enable continuous or repeated observations that were previously only attainable in clinical settings. IoT-enabled home devices can monitor environmental triggers and adherence to therapies. When combined with analytics, these streams can support risk stratification algorithms that identify deterioration earlier than sporadic clinic encounters and that prioritise interventions to avert acute episodes. In principle, for low-income populations the downstream effects are attractive: fewer emergency admissions, fewer invasive procedures, and reduced catastrophic out-of-pocket expenditure tied to hospitalisation. This is why these technologies can perform both as clinical aids and socioeconomic equalisers.

However, the promise of IoTs and wearables becomes complex and open to contest when the data they generate are folded into contractual relations with insurers, creating a new sector named INSoT, the Insurance of Things.

The pandemic [81] accelerated public awareness of health risks and contributed to growth in consumer demand for protection against health-related expenditures. [82] So, insurers, responding to market dynamics, have deepened their engagement with digital health tools integrated in the policies: they started proposing schemes that explicitly leverage behavioural and biometric data to shape cover and price. In the depicted scenario, insurance companies have introduced a range of IoT/wearables integration into policy models: discounts on premiums conditional on engagement with wellness programmes, subscription or membership benefits tied to device use, provision of devices or services for free or at subsidised cost in exchange for data sharing, vouchers or rewards for sustained healthy behaviours, and tiered products that adjust underwriting rules based on continuous monitoring.[83]

This integration produces a perturbative effect on the mentioned HI contract. Traditionally, insurance underwriting begins with an assessment of the applicant: a one-off evaluation of personal, medical and behavioural factors used to classify risk through a questionnaire and set a fixed premium, like a photograph of the policyholder. That model assumes a relatively stable risk profile that can reasonably be summarised at inception and adjudicated through defined policy terms. By contrast, embedding IoT devices and wearables into the insured relationship replaces or combines that initial, static mapping with a continuously evolving dataset generated by real-time monitoring. Consequently, risk assessment shifts from a point estimate to a dynamic process. Premiums, coverage conditions and incentives may be recalibrated in response to live data streams rather than remaining anchored to the original underwriting file. Insurers can observe behavioural and physiological signals on an ongoing basis and adjust their view of exposure accordingly. This creates a contractual regime where obligations and benefits are contingent on future measurement, producing novel uncertainties for both parties.

4.1. AI-driven contracts implications.

The mentioned perturbation of the private law contract has multiple direct and indirect implications.

This reconfiguration challenges the traditional actuarial framework by introducing temporal volatility and potential feedback loops between monitoring, behaviour and underwriting.

Precisely, the above-mentioned integration of automation and monitoring in contracts impacts on bilateral informational asymmetry.[84] Policymakers may

[81] P Thottempudi and others, 'Digital health resilience: IoT solutions in pandemic response and future healthcare scenarios' (2025) 6 Discover Sustainability 144.
[82] Battelli (n 12) 83.
[83] A Spender and others 'Wearables and the internet of things: considerations for the life and health insurance industry' (2019) 24 British Actuarial Journal 1-31.
[84] F Greco, 'Trasparenza e obblighi comportamentali' in M Gorgoni, F Greco (eds.) *Diritto delle Assicurazioni* 395-414; Soleymanian, Weinberg, Zhu (n 34) 231. It is worth mentioning that the informational (and

not fully understand the risks, but most of all policyholders may not fully understand how continuous data will affect their terms. Policyholders may not realise the impact of poor maintenance, poor device monitoring, inaction during periods when they are working or have other commitments, and the extent of the data set that is collected.

A second innovative profile emerging from the integration of IoTs and wearables into HI is the temporalisation of underwriting and contract duration. Rather than treating risks as a static attribute measured at inception, insurers are now able to observe continuous behavioural and physiological streams and to make coverage contingent on trajectories over time. Devices that record activity patterns, sleep quality, heart-rate variability, glucose excursions or medication adherence enable insurers to define eligibility and benefit levels not only at the point of sale but throughout the lifetime of the policy. This produces contract forms in which renewal, premium adjustment and scope of cover are functions of longitudinal metrics: a sustained period of "healthy" readings may trigger discounted renewal offers, whereas an unfavourable trend could provoke premium increases, additional co-payments or conditional cover windows. Such arrangements, known as "pay as you live" or "cover as you need" models,[85] are "usage-based insurance" schemes (UBI)[86] which nominally tailor financial exposure to actual behaviour and health status. This appears to be a contract configuration method compatible with the so-called best execution rule,[87] according to which the insurer must take steps to provide the customer with the best possible contract, tailored to their specific needs. In practice, however, they transform the contract from a stable social instrument into a continuously negotiated bargain mediated by data flows, shifting risk assessment into an operational, ongoing activity.

A third innovative profile is the emergence of surveillance-driven exclusion and pre-emptive contract termination. Continuous monitoring can reveal early, subtle signs of disease that the user may not understand or appreciate because of informational asymmetry; insurers, by contrast, possess analytic capacity to detect and act on these signals. When contractual terms permit, such inferences may be used to restrict or withdraw coverage before clinical diagnosis or before the patient has had an opportunity to seek appropriate care. The consequences can be listed as follows: denied or limited cover increases out-of-pocket exposure precisely for those entering a trajectory of increasing need, thereby impeding access to costly but necessary

bilateral) asymmetry is also a issue in traditional insurance policies, as considered by Battelli (n 12) 83; A Zurlo, 'L'oggetto del contratto di assicurazione', in M Gorgoni, F Greco (eds.), *Diritto delle Assicurazioni* 157 ff.; D Porrini, 'Asimmetrie informative e concorrenzialità nel mercato assicurativo: che cosa cambia con i Big data?' (2016) Concorrenza e mercato 139 ff.; M Chironi, 'L'accordo, la forma e la durata del contratto' 128.

[85] These schemes mimic the the plethora of contracts that have emerged for motor insurance: "pay as you drive" or "pay how you drive". On the matter see, M Infantino, D Porrini, 'Portabilità dei dati e scatole nere. un commento a margine di una recente riforma' (2025) 2 Resp. civ. prev. 672.

[86] Soleymanian, Weinberg, Zhu (n 34) 229 ff.; E Battelli, 'Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi' (2019) 12 Corr. Giur. 1517-1518; MC Gaeta, D.S. D'Aloia, 'InsurTech in Italy: opportunity, risks and applicable regulation' (2021) 2 European Journal of Privacy Law and Technology 19.

[87] M Rossetti, *Il diritto delle assicurazioni. Vol. I. L'impresa di assicurazione. Il contratto di assicurazione in generale* (Pacini Giuridica 2011) 854 ff.; Zurlo (n 84) 166.

interventions. This dynamic disproportionately affects socioeconomically vulnerable individuals who rely on insurance to manage catastrophic costs.

Moreover, the spectre of surveillance-based penalties fosters risk-averse behaviour and may undermine therapeutic self-determination: patients may avoid seeking diagnostic care, clarity, or even decline beneficial interventions since they fear of incurring adverse contractual consequences. In both profiles, the promise of personalised, adaptive coverage is shadowed by new forms of conditionality and exclusion. To prevent it, the surveillance should be converted as a new configuration for the "rescue burden" (onere di salvataggio), according to art. 1914, co. 1, c.c., to prevent damages and limit the negative externalities.[88]

This reconfiguration of the rescue burden can have a decisive impact on the market: statically estimated insurance costs lead to the selection of only high-risk individuals, while those who fall into a low-risk cluster usually decide not to take out insurance because of the cost, causing a phenomenon known as the Akerlof adverse selection. [89] In addition, policyholders engage in riskier behaviour, known as moral hazard. In contrast, parametric insurance is structured to cover low-risk individuals and prevents moral hazard, although the literature[90] emphasises the innovative scope of these measures to include even the most serious and chronic patients in the market.

Furthermore, while it is true that scientific and legal literature[91] asserts that this insurance model, which integrates monitoring with wearables, would make it possible to insure a larger number of people, especially those with chronic conditions or illnesses who have limited access to these contracts, it is also true that data collection can lead to an initial negative assessment that discourages policymakers from insuring the sick person, thus determining a sort of mutation of the insurance contract devoid of its typical mutualistic risk.[92]

Additionally, the data driven nature of the profiling for the risk pooling interferes with the application of the policyholder duty to provide duly information to let the policymaker choose the adequate "bucket" in risk pooling.[93] This reversal generates a disruption of communication flows and of the legal dynamics envisaged by statutory provisions. If so, informational paucity or opacity cannot be imputed to the policyholder, whose informational corpus may have been supplanted by IoT outputs. Attention instead turns to whether reliance on inappropriate datasets can be attributed to the policymaker. That question is especially acute where regulatory frameworks allocate communicative duties between policyholders and policymakers in a

[88] On the rescue burden, see Santagata (n 12) 167; Zurlo (n 84) 173 ff.; Partenza, Nucci (n 53) 32-34.
[89] Maggiolino (n 72) 95.
[90] Keller (n 46) 3.
[91] C Poncibò, P Terezkiexcz, 'EU Digital Insurance: Comparative Legal Perspectives' (2025) 14 AIDA Europe Research Series on Insurance Law and Regulation <https://doi.org/10.1007/978-3-031-96496-1_1>; A Spender and others, 'Wearables and the internet of things: considerations for the life and health insurance industry' (2019) 24 British Actuarial Journal 1-31.
[92] Battelli (n 12) 85; Manes (n 71) 485.
[93] Manes (n 71) 474; Gürses (n 49) 542: according to the A., the essence of the duty of fair presentation of the risk lies on the tests of materiality and inducement (…). The data that the insurer has taken into account has therefore to be revealed by the insurer who would argue that the assured breached the duty of fair presentation of the risk. The insurer who argues the breach of the duty would have to specifically identify the issues known by the insurer through the data already available to them and the information provided by the assured, as well as the circumstances that the assured failed to present fairly.

way that presumes reciprocal access to reliable information. The problem is compounded when the policymaker exerts only limited control over the dataset, or when a third-party provider curates and governs the datasets.

It is possible to also note that profiling is feasible because insurers rely on large, heterogeneous and regularly updated datasets, which enable risk stratification and predictive modelling. The core issue, however, is that datasets often embed structural biases related to gender, disability and ethnicity. Women, people of colour and individuals with rare diseases or disabilities are frequently under-represented in research, producing sparse and skewed data first and wrong "bucket" risk pooling later.[94] Such gaps distort model outputs, perpetuate discriminatory inferences and undermine the fairness and legality of profiling practices embedded in the insurance contract.

Taking into account the mentioned implications, one must consider the contract is void whenever it covers for a risk that cannot be covered for, like the costs intentionally caused by the insured, according to art. 1900 c.c. Since the insured person has wearables, they can prevent medical expenses by leading a healthy lifestyle: if the person benefiting from a parametric insurance contract has a lifestyle that is not compatible with the goals set or the average standards for their category, then the illness or expense to be reimbursed could be considered as voluntarily created, and therefore not subject to coverage because it is not insurable. This is not true if we only consider that the subject is not always able to understand the consequences of the relationships that arise from that data, because they do not have the wealth of information available to the doctor, clinic or insurance company.

Also, since the contract is based on continuous data monitoring, it does not seem to comply with the principles that govern indemnity insurance. The insured policyholder pays a fixed amount for the medical expenses' coverage upon the occurrence of an eventual triggering event. So, instead inherently data driven insurance policies could recall an "index" based product,[95] where the payment is determined by the degree of covariation between an event and an estimated loss. While the main principle for insurance is that the assured is entitled for indemnity (art. 1882, 1904, 1905, 1907, 1908, co. 1°, 1909 and 1910, c.c.), [96] up to the full amount of the actual loss suffered, whenever the parametric insurance interferes with this principle, the contract cannot be considered insurance, but it is an index-based product, which may obey to other disciplines. If these pacts do fall into the parametric or index-based contract framework, then they need to comply with art. 37 EU Regulation no. 1305/2013 and art. 2-bis d. lgs. 102/2004. Notwithstanding, to apply this framework to a parametric pact, it is required that the payment is subject to an objective exogen index. However, the contract considered in this paper is certainly parametric in the sense that it depends on the tracking of specific data on which the determination of risk depends, but prima facie they do not appear to be either objective or external. They are not objective because they relate to the person insured by the policymaker; they are not external because they can be

[94] K Langenbucher, 'Responsible A.I. Based Credit Scoring – A Legal Framework' (2020) 31 European Business Law Review 527-547.
[95] In this sense, Gürses (n 49) 537. The A. argues that the term insurance is misplaced.
[96] Santagata (n 12) 138.

controlled through suggestions and tracking by the policymaker and are undoubtedly subject to influence by the policyholder who produces this data. If anything, this index can be assimilated to external and objective indices if we consider the black box effect, the asymmetry and the inability of the insured to understand the implications of the collection of this data. Therefore, the parameter must necessarily be customised for risk pooling, it performs a technical function of verifying that the threshold for coverage has been reached, it is connected to the interest of the insured to be reimbursed, and so it can be inferred that the insurance in question is not subject to the rules laid down for contracts directly linked to index or units of collective investment undertakings referred to in art. 41 Insurance Code.[97] Moreover, this peculiar model of health insurance appears to reconfigure the category of the estimated insurance policies, according to art. 1908 co. 2 c.c.: since the estimated risk is limited by the data collected, and coverage is determined by reference to the expenses actually incurred or to be incurred, or by the cost of the healthcare service requested from the hospital. However, in practice, it will be necessary to verify whether the index is always internal or external and whether the reimbursement serves an indemnity or speculative function, to identify the applicable regulations.

The above-mentioned control intersects and broaden the product oversight and governance (POG):[98] on one end, the policymaker do need to walk through a process for the product approval; on the other, they have the duty to evaluate a coherent and adequate risk profile to the target client and to do it in a transparent way, according to the EU Directive 2016/97 and d. lgs. 68/2018.[99] Finally, the use of monitoring and the anchoring of contractual risk may result in the loss of the aleatory nature of the contract itself.[100] Thus, the loss of intrinsic uncertainty, which determines the need to allocate risk to others, may lead to a void contract, unless the risk assessment is not based exclusively on continuous profiling but is anchored also to an initial static profiling that offers coverage regardless of the data collected.

4.2. The premium narrative.

Scientific literature [101] has focused and continues to focus on the consequences of exchanging data for services or money for services. As will be

[97] In questo senso, si veda R Santagata (n 12) 141; *contra* Ö Gurses, 'Insurance Law and AI. Demystifing InsurTech', 537.

[98] A Camedda, 'La product oversight and governance nel sistema di governo societario dell'impresa di assicurazione' (2021) 2 Banca Borsa Tit. Credito 234 ff.; Hazan (n 12) 75.

[99] S Landini, 'Appropriatezza, adeguatezza e meritevolezza dei contratti di assicurazione' (2017) Assicurazioni 39-58; Santagata (n 12) 163. On the broadened application of the suitability rule, see M Hazan, 'L'assicurazione "responsabile" e la responsabilità dell'assicuratore: quali prospettive dopo IDD?' (2017) Danno e resp. 630 ff., who states that IDD broadened the concept of suitabily, taking into account not only the specifics of the single contract (and client) but also the specifics of the market in which the product is sold.

[100] Battelli (n 86) 1519.

[101] C Langhanke, M Schmidt-Kessel, 'Consumer data as consideration' (2016) 5 Journal of European Consumer and Market Law 218; A De Franceschi, *La circolazione dei dati* (ESI 2017) 67 ff.; A Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?' (2018) Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 7, 1 ff.; G Resta, V Zeno-Zencovich, 'Volontà e consenso nella fruizione dei servizi in rete' (2018) Riv. trim. dir. e proc. civ., 411, 436 ff.; V Ricciuto, 'La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno' (2018) 4-5 Il

assessed below, data processing regulations do not exclude this possibility and the tying of consent to a contract for the desired service.

Nevertheless, the object of this paper analysis appears to be somewhat different. In the contracts analysed, i.e. AI-driven HI contracts, consent to data processing is not exchanged for access to a free service: the service is paid for, but data are provided to gain a reduced rate or to get access to additional services or even to get exclusive packages. This constitutes a middle ground narrative compared to that studied in the literature on data processing, namely the premium narrative.

Two question then arise: is it the exchange data for cover allowed and within which circumstances? Does the exchange between the premium package and consent have further implications? While the first question will be addressed in the following paragraphs,[102] the second question opens the way to further reflections, because premium narratives can not only contribute to undermining individuals' self-determination in healthcare, data processing and insurance agreements, but can also generate additional problems for consumer protection. In fact, this way of reconfiguring the contracts analysed risks introducing unfair commercial practices, such as gamification.

Gamification[103] is the application of game design elements, such as points, badges, leaderboards and progress bars, to different contexts not linked to recreational functions to motivate and engage people, turning routine tasks into more rewarding experiences. Common examples include loyalty schemes, fitness apps that use streaks and badges to encourage exercise, corporate training platforms that award points for completed modules, and social apps that use leaderboards to increase interaction. Educational platforms add quizzes and levels to improve retention, while some civic initiatives use gamified challenges to boost participation in surveys or recycling programmes.

This practice does not only apply to recreational contexts, such as the video game or sports industries,[104] instead gamification consists in the application of games and related strategies to various other sectors , including finance[105] and potentially insurance. The phenomenon enables the user to boost participation and learning, especially among younger and first-time users, it can allow providers to build loyalty and trust, but it carries risks. These systems may encourage superficial engagement or "gaming the system", where users chase rewards rather than meaningful outcomes, and can undermine intrinsic

diritto dell'informazione e dell'informatica 689; S Thobani, 'Operazioni di tying e libertà del consenso' (2019) Giur. it. 533 ff.; id., Processing Personal Data and the Role of Consent (2020) European Journal of Privacy Law and Technologies 93-104, in particular 96; id., 'Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente' (2019) Media Laws 147; id., 'Il consenso nella regolazione della circolazione dei dati' (2025) 2 Persona e Mercato 469-486; V Bachelet, *Il consenso oltre il consenso. Dati personali, contratto, mercato* (Pacini Giuridica 202) 51 ff.; G Versaci, *La contrattualizzazione dei dati personali dei consumatori* (ESI 2020) 69 ff.; Rapisarda (n 15) 201.

[102] *Infra* § 5.

[103] A Faust, *The effects of gamification on motivation and performance* (Springer Gabler 2022); V Zambrano, 'We are only scratching the surface: a proposito di ai e sfruttamento economico dei dati sportivi' (2025) 2 Contratto e impresa 299-332.

[104] On the matter, it is possible to read a first assessment of gamification in the sport and game industries provided by the Italian case law: Trib. Torino, sez. Impresa, 11 october 2023, n. 3872; Trib. Torino, sez. III, 11 october 2021, n. 4523.

[105] C Brescia Morra and others, 'La gamification degli investimenti finanziari' (2025) 32 Quaderni giuridici, 7-98, available at: <https://www.consob.it/documents/d/area-pubblica/qg32>.

motivation, create unhealthy competition, or even foster addiction-like behaviours.

Gamification can create a cognitive bias for the user[106] and especially for contractual parties: who concludes the contract does it for its playful nature or accesses the premium version or other accessories and services for its playfulness or remains bound by the contract or decides to continue to sign the contract for its playfulness or underestimates the negative externalities of the contract because they are described to the contractor as a loss in the game and not as an economic loss or downplays the losses.[107] Also, the practice can be linked to social media trends and the proliferation of financial influencers, often referred to as fin-influencers, producing a phenomenon known as behavioural contagion, with uncritical, imitation based, and herd-like adherence by consumers based on informational cascades, i.e. the herd effect. For these reasons, a contract can be signed because it is a viral trend to do so and not because the party (especially the vulnerable and weaker one) understood the severity of the negotiation. It appeals to younger and first-time consumers, also due to emotional or aesthetic reasons.

While in other sector gamification hasn't been assessed by authorities and the national case law, it has been legally assessed and framed into legal categories in the gaming and financial sectors.

In the gaming sector, gamification is referred to be a harmful action in games and videogames, as provided by the European Commission's Consumer Protection Cooperation Network (CPC), [108] and it is considered to be, potentially and according to the specific case scenario, an aggressive or deceiving practice against consumer rights, according to AGCM.[109] It is an unfair practice even if the prize or reward is assigned casually to the consumer.

To qualify gamification as unfair practice can lead to different consequences. First, it poses greater attention to pre-contractual disclosure requirements, not so much for reasons related to data protection or the suitability of insurance products, but for the protection of vulnerable consumers. Second, since these activities could be addressed as unfair practices, art. 18 co. 1 lett. m) of the Italian Consumers Code applies: the competent administrative independent authority (AGCM) has a surveillance duty on the sector, can adopt emergency measures, has powers to inhibit the continuation of the activity, also has the power to make the sanction public in order to inform consumers of the nature of the practice and prevent the negative effects of its possible continuation. Furthermore, consumers who have been harmed by unfair commercial

---

[106] C Failla, 'Gamification, dark patterns e cripto-attività. Prospettive di adattabilià della disciplina delle pratiche commerciali scorrette' (2024) Osservatorio del diritto civile e commerciale, 114; A Mathur, J Mayer, M Kshirsagar, 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods' (2021) Conference on Human Factors in Computing Systems, 3-5; A Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACMon Human Computer Interaction 2.

[107] Brescia Morra (n 105) 10.

[108] European Commission, *Commission and national authorities take action to protect children from harmful practices in video games*, Brussels, 21 march 2025, available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_831>.

[109] AGCM, 19 october 2020, n. 28368, proc. n. PS11593. On the matter, see A Fachechi, Gli orientamenti dell'Autorità Garante della Concorrenza e del Mercato in materia di pratiche commerciali scorrette (2019-2020) Conc. merc. 26-27, 543-554.

practices may also bring proceedings before the Italian competent ordinary courts to obtain compensation for the damage suffered and a reduction in price or termination of the contract, taking into account the seriousness and nature of the unfair commercial practice, the damage suffered and other relevant circumstances, in accordance with Article 27, co. 15-bis of the Italian Consumer code.
In the financial sector, after the notable cases of Gamestop and Trade Republic AG,[110] new regulations have been adopted. Art. 22 co. 1 law no. 21/2024 modified art. 7-*octies* co. 1-*bis* of the Unified Code of Finance (TUF), which now bans internet advertising of financial products, activities and services, even when considered indirectly, whenever the investment is promoted by an unauthorised person. Moreover, this practice could be addressed as market manipulation, with the related administrative and criminal sanctions.

5. AI-driven HI and Data Protection.

The mentioned contractual hybridisation now raises several critical issues, connected to data protection.

Monitoring technologies deployed by insurers capture a wide range of personal information, from daily habits to precise geolocation, yet the accuracy and meaning of such data are contingent on how devices operate, on user maintenance and on technical limitations. Devices frequently lose data, misclassify activities and fail to reflect contextual factors or external influences that shape human behaviour, so continuous profiling premised on seamless surveillance is factually and technically flawed. The reliance on this imperfect data gathering risks entrenching inequality: individuals who already face barriers to traditional cover, such as those with chronic conditions, are pressured to surrender detailed personal information simply to obtain or afford insurance, producing a commodification and datafication [111] of vulnerability. For those who lack technological literacy or resources, this dynamic effectively creates a "data for cover" market in which the poorest exchange privacy for access to services,[112] while an opaque surveillance-capitalism model operates behind subscription-style premium reductions. In these HI schemes, data can be seen as part of counter-performance, jointly with the payment of the premium price or discounted subscription price. It is a model that fosters a form of participation surveillance[113] where consent is given under asymmetrical power and informational disadvantage, undermining the voluntariness that data protection law presumes.

Moreover, the gamification techniques embedded in some schemes incentivise behavioural modification in ways that may be discriminatory or coercive, and they open pathways to punitive uses of data: adverse adjustments to premiums, denial of renewal, or the generation of risk scores

[110] On the Gamestop and Trade Republic cases, see Brescia Morra (n 105) 14-22.
[111] F Gattillo, 'Assicurare l'opera d'arte digitale: rischi emergenti, polizze cyber e nuove tecnologie' (2024) 2 Arte e diritto 347 ff.
[112] On the use of personal data as a counter-part performance or an exchange, see Langhanke, Schmidt-Kessel (n 101) 218; De Franceschi (n 101) 67 ff.; Resta, Zeno-Zencovich (n 101) 436 ff.; Ricciuto (n 101) 689.
[113] Germani, Ferola (n 43) 75.

that follow individuals into other domains. This also affect a constitutional right, such as self-determination in medical treatments.

The cross-sectoral effects are several: scoring[114] resulting from insurer-held telemetry can influence access to other insurance products, employment opportunities and credit, amplifying systemic exclusion.

These factors explain why health data collected by mobile applications,[115] Internet of Things devices and wearable technologies, are firmly regulated under the General Data Protection Regulation (EU) 2016/679 [116] and the emerging framework established by Regulation (EU) 2025/327[117] .

Insurers seeking to employ these data streams for risk management cannot treat them as ordinary telemetry: instead, their processing must rest on a clearly articulated lawful basis, with explicit, freely given and revocable informed consent where that basis is relied upon and must satisfy the GDPR's core principles of purpose limitation, data minimisation, accuracy and storage limitation. These legal constraints are complemented by the governance structures and technical requirements of Regulation 2025/327. This consent also provides an additional level of information pursuant to Article 119-*bis* of the Italian Private Insurance Code.[118]

The General Data Protection Regulation introduced a clear framework to enable a firm personal data protection towards exogenous incursion but also provided a right to data portability under Article 20,[119] to allow individuals to receive their personal data in a structured, commonly used and machine-readable format and to transmit those data to another controller. This right was conceived to facilitate the circulation of personal information across services and borders, thereby supporting contractual engagement while preserving the data subject's autonomy through consent. Portability under the GDPR, however, is anchored firmly to the individual's control: processing for portability relies on a lawful basis such as consent, and where consent is invoked, it must be specific, informed, freely given and revocable. High standards of confidentiality and security accompany this right, reflecting the

---

[114] Manes (n 71) 469-471. The A. notes that, in the area of access to credit, the Italian legislator was prompted by the European legislator and has adopted regulations that allow policymakers to map information on policyholders and, where necessary, query the relevant database in order to protect the credit system. This possibility would lead to improve the risk assessment phase and lower risk exposure, but, at the same time, this would also increase the costs that policymakers have to bear for risk assessment, making this reconfiguration unlikely to be adopted on a large scale of contracts. On the high costs of these products, see also Santagata (n 12) 169.

[115] Rapisarda (n 15) 187 ff.

[116] The literature on the matter is quite extensive, for this reason see G Finocchiaro, 'Introduzione al Regolamento europeo sulla protezione dei dati' (2017) Nuove leg. civ. comm. 1-18.; id. (ed.), *La protezione dei dati personali in Italia, Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* (Il Mulino 2019).

[117] A Morace Pinelli, 'Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)' (2025) 4 Nuova Giurisprudenza Civile Commentata, 1016-1031; M Faccioli, 'La responsabilità civile per violazione della disciplina per l'utilizzo dei dati sanitari elettronici nell'European Health Data Space (art. 100 Reg. 2025/327/UE)' (2025) Resp. civ. prev. 5; S Faillace, 'I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo regolamento EHDS' (2025) 2 Contratto e Impresa 379-401; S Corso, 'Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327' (2025) 3 Nuove Leggi Civili Commentate 563-603; id., 'Il trattamento dei dati personali in ambito sanitario' (2025) 2 Riv. it. informatica e diritto 2-20; F Cascini, MA Arcuri, 'Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale' (2024) 6 Diritto dell'informazione e dell'informatica 837 ff.

[118] Greco (n 84) 398-400.

[119] On the matter, see M Infantino, D Corapi, 'Portabilità dei dati e scatole nere. Un commento a margine di una recente riforma' (2025) 2 Resp. Civ. Prev. 672 ff.; Battelli (n 86) 1520.

GDPR's special protection for health-related information as a peculiar category of personal data.

Recent regulatory developments, notably the European Health Data Space Regulation 2025, partially affect and modify this paradigm.[120] Especially after the Covid-19 pandemic, the EU wants to stress and enforce the centrality of individual data control and the growing societal importance of health data for research, planning and the economy, as well. This is why 2025 EHDS introduces a two-track model. The first track preserves primary use under the familiar consent-based and patient-centred regime: personal health data used for direct care or under explicit consent remain subject to individual authorisation and the associated safeguards. The second track creates a regulated pathway for certain secondary uses of health data without requiring individual consent when processing serves clearly defined objectives of public interest. More precisely, art. 53 EHDS[121] enumerates broad categories of such purposes, including scientific research, public health surveillance and health system planning. A similar provision entered into force in Italy, thanks to the new Italian law on AI applications, art. 8 l. 23 settembre 2025, no. 132.[122] Nevertheless, art. 24 lett. B) Law no. 132/2025 provides for a regulatory framework and delegates powers to the Italian Government to update regulations in the banking, insurance and payment services sectors in accordance with the regulation.

To the purposes of the analysis of this paper, careful consideration must be placed when comparing the different definitions.

On one end, the GDPR's notion of health data[123] is intentionally broad, covering any data that reveal health status, including derived or inferred indicators.[124] Furthermore, if the provisions of the GDPR are specified considering the DSA, health and wellness products are medical devices regulated according to the functionality of the product, as intended by the manufacturer. The device will be a medical device if the intended functionality of the device has a medical purpose, including, for example: actions such as diagnosis, prevention, monitoring, prediction, prognosis, treatment, mitigation, investigation, replacement or modification relating to a disease, injury or disability, or the anatomy of a physiological or pathological process or condition; the provision of an in vitro examination of samples from the human body; and the control or support of conception.[125]

---

[120] Morace Pinelli (n 117) 1018-1019; Faillace (n 117) 382; Corso (n 117) 586.
[121] Morace Pinelli (n 117) 1020; Faillace (n 117) 381, fn. 4.
[122] Legge 23 settembre 2025, no. 132 recante le *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, published in G.U. 25 september 2025, no. 23.
[123] Rapisarda (n 15) 195; E Giusti (n 15) 85 ff.
[124] Art. 75 of the Italian Privacy code recalls the same notion and the same terms for legal treatment. On the notion provided by art. 75, see D Poletti, 'Commento sub art. 75 D.lgs 196/2003', in CM Bianca, FD Busnelli (eds.), *Commentario al codice privacy 2003* (Cedam 2007) 1205; P Guarda, 'I dati sanitari', in V Cuffaro,R D'Orazio, V Ricciuto (eds.), *I dati personali nel diritto europei* (Giappichelli 2019) 597. Moreover, this notion has been interpreted in a broader sense whenever standard data can have an identification pattern for the user and impact health: on the matter, see Cass. civ., Sez. Un., 27 dicembre 2017, n. 30984, in *Giur. it.*, 2018, 12, c. 263, con nota di A Ricci, 'Protezione dei dati personali-trattamento di dati sensibili e principio di responsabilizzazione'.
[125] A Dennis, 'Healthcare technology regulation in the EU and the UK: from medical devices to intellectual property and advertising', in J. Madir (ed.) *HealthTech: Law and Regulation* 53-79.

On the other, the EHDS adopts the terminology of Article 14 to specify the forms of electronic health data that are subject to access and exchange regimes: these are typically records and clinical data held within healthcare systems. Notably, data generated by consumer Internet-of-Things devices, wearables and wellness apps are not automatically encompassed by the EHDS list, unless they are incorporated into clinical records under the secure clinical exchange framework. Interoperability rules permit such an intersection: data from an app or wearable may become part of an electronic health record if accompanied by the regulation's conformity label, if it is integrated through established clinical exchange channels, if a specific consent has been provided.

So, across all applicable instruments, consent for processing data originating from wearables, IoTs and apps still remains central. Although there is marked support within the EU for circulation and secondary use without consent, the use of data for marketing purposes remains unrelated and therefore insurance companies cannot resort to regulatory innovations to justify its processing. Where consent is the lawful basis, it must be explicit, specific, informed and freely revocable; the data subject must be able to withdraw consent at any time, and withdrawal must have practical effect, ceasing further tracking or processing.

The above-mentioned centrality of informed consent requires to consider revocability holds even where an individual's insurance coverage or underwriting model relied on continuous data feeds. If consent withdrawal requires to terminate the data flow, the monitoring through IoT and wearable must cease, although the contract is based on a dynamic monitoring of the policyholder.

These regulatory contours produce several consequential implications for insurers and other commercial actors that seek to rely upon app, IoT and wearable-derived health signals in risk management and contractual design.

First, there is an intrinsic restriction on the applicability of a contractual model premised exclusively on continuous tracking. Because individual consent to processing remains protected and revocable, a contract that depends solely on uninterrupted tracking cannot be guaranteed in perpetuity. The policyholder retains the right to withdraw consent, thereby interrupting the data flow upon which the contractual performance may have been predicated. This feature constrains the space for purely tracking-based contractual formulations even where portability and data exchange facilitate initial contractualization. This is why insurance analysis considers legislation and data protection as the first barriers for this new insurance reconfiguration.[126]

Second, if considered viable as a contract depending on the wearable and IoT data processing, withdrawal of consent to monitoring cannot lawfully produce automatic termination of an insurance contract where such termination would coerce the insured into sustaining monitoring against their will. To treat revocation as a ground for contract dissolution would instantiate a de facto compulsion to consent, incompatible with the GDPR's insistence on voluntariness and with fundamental principles of contract law that prohibit unlawful tying of a right to the surrender of autonomy. Accordingly, a tying

[126] D Neumann, V Tiberius, F Biendarra, 'Adopting wearables to customize health insurance contributions: a ranking-type Delphi' (2022) 22 Medical Informatics and Decision Making112; Vigil Iduate (n 49) 176.

relationship[127] between consent to tracking and the insurance contract may exist in relation to privileges, discounts or tailored terms, but the exercise of the right to withdraw consent shouldn't extinguish the policyholder insurance coverage. Therefore, ultimately it should be noted that the practice of tying is not prohibited per se but it is permitted only in cases where the service is offered either for a fee or free of charge in exchange for consent to processing. Furthermore, the paid service and the service accessed by consenting to the transfer of data must be equivalent. Finally, it must be possible for the service covered by the contract to be provided by the data controller without the need to consent to further or additional uses of the data.

Third, if monitoring functions as an index correlating to the level of coverage, premium or additional benefits, the decision for cessation of monitoring legitimately gives rise to contractual adjustments rather than automatic termination. The reasonable legal architecture is one of renegotiation or the application of a default or standard tariff in place of monitoring-linked advantages. Such an approach preserves the insured policyholder's autonomy while allowing insurers and policymakers to recalibrate risk allocation and pricing considering diminished information. Only by taking this path, it is possible to prevent the risk or the predicted risk for diminished protection for individuals who might otherwise be uninsurable or charged prohibitive rates, notably those with chronic conditions, while maintaining the high standards of privacy and data protection demanded by EU law.

It should also be considered that individual scoring is a further cause for concern for European legislators, which in the GDPR has resulted in the obligation to explain creditworthiness decisions when they are based on algorithms that are not comprehensible to the individual.[128] The aim is to prevent the "black box" effects of intelligent predictive systems. This seems to refer exclusively to access to credit and not to insurance coverage; nevertheless, a strengthening of the information obligation in the pre-contractual phase and during the execution of the contract can be recovered with the suitability rule,[129] under MiFID II EU Directive 65/2014, Insurance Distribution Directive 97/2016 and art. 183 co. 2 of the Italian Private Insurance Code.[130]

However, the European Union's efforts to regulate new technologies applications continue. Considering the ongoing drafting of the Digital Fairness Act (DFA), the European Commission recently published the findings of the Digital Fairness Fitness Check. The DFA would aim to fill the regulatory gaps left by earlier landmark digital laws, such as the Digital Services Act and Digital Markets Act, as well as structural consumer protection frameworks and

[127] S Thobani, 'Operazioni di tying e libertà del consenso' (2019) Giur. it. 533 ff.; id., 'Processing Personal Data and the Role of Consent' (2020) European Journal of Privacy Law and Technologies, 93-104, in particular 96; id., 'Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente' 147; id., 'Il consenso nella regolazione della circolazione dei dati (2025) Persona e Mercato, 2, 469-486; Bachelet (n 101) 51 ff.; G Versaci, *La contrattualizzazione dei dati personali dei consumatori* (ESI 2020) 69 ff.; Rapisarda (n 15) 201.
[128] Manes (n 71) 481.
[129] Landini (n 99) 39-58.
[130] Zurlo (n 84) 166.

safeguards, including the Unfair Commercial Practices Directive, Consumer Rights Directive, and Unfair Contract Terms Directive. Namely, the DFB would target business-to-consumer (B2C) practices across interface design, subscription management, personalised pricing and marketing strategies, and influencer-led content in digital environments. According to the mentioned Fitness Check, a wide range of harmful online practices has been identified, including "Sneak Into Basket", confirm shaming, forced continuity, hidden costs, unknowingly granting permissions, bait and switch, misdirection, disguised ads, shadow banning, buried data sharing, and most of all subscription with dynamic pricing, particularly when algorithmic or behavioural design methods disproportionately impact vulnerable consumers, including minors, older persons, and individuals with lower education levels. It is worth mentioning that the EU Legislative process is still in the making, and by 2027 AI driven contracts with subscription with dynamic pricing could be heavily affected and even restricted by new consumer-protective policies.

So, the various European disciplines engaged with algorithmic contracting and parametric insurance increasingly converge on three core priorities: strengthening transparency and information duties, widening the scope of the suitability rule, and recognising informed consent as the decisive authorisation for AI-driven contractual mechanisms.

The recent Italian legislative efforts exemplify this trajectory and add operative detail. Notably, art. 20 Law 16 December 2024, no. 193[131] addresses market competition in automotive insurance by prohibiting contractual clauses that prevent the policyholder from uninstalling electronic mechanisms upon contract expiry. This provision operationalises transparency and consumer autonomy, limiting residual vendor lock-in and supporting post-contract mobility. The policyholder can have access to the gathered data, and the policymaker can use the gathered data to calculate the premium and even to continue or discontinue the insurance coverage. Whenever the insurance company wants to terminate the contract because of the data, then the policymaker needs to compensate the policyholder, with an amount of 20 euros.

6. Conclusion.

In contexts of poverty affecting millions of Italians and shaping medical decision making, the diffusion of eHealth and mHealth represents a potential turning point for access to care and health management. Yet, this technological promise is shadowed by significant risks arising from the convergence of parametric insurance, medical practice and pre-existing vulnerability, therefore «technological progress has merely provided us with more efficient means for going backwards».[132]

[131] On the new relevant legislation for the automotive sector, see Infantino, Porrini (n 85) 672. On the impact of automation in the automotive sector, see S Pellegatta, 'Automazione nel settore automotive: profili di responsabilità civile' (2019) 4 Contratto e impresa 1418-1446.

[132] A Huxley, *Ends and means: An Inquiry into the Nature of Ideals* (Harper & Brothers 1937).

At a time when the practical force of informed consent and individual autonomy appears increasingly eroded [133] by automated processes and datafication, normative references nonetheless reassert the centrality of information and consent as legal and ethical anchors. Even where regulatory regimes open avenues for the circulation of data without explicit consent, including data directly related or indirectly related to health, the principles of transparency and self-determination must be actively safeguarded.

The above-mentioned imperative holds irrespective of the technical complexity of intelligent systems, the multilayered and evolving nature of the regulatory framework, and the demonstrable capacity of algorithmic tools to influence individual behaviour. Protecting autonomy cannot be traded away in exchange for convenience, discounts or premium subscriptions embedded in health-insurance contracts. Crucially, such contracts must be preceded by the execution of the information obligation, capable of satisfying the suitability rule, the data protection regulation and the consumers' rights policy. Especially considering transparency and informed consent, the short duration of the contract and the new guarantees introduced by Law no 193/2024 for the automotive insurance sector, including the right of access and control of tracked information, as well as the right not to use the device for monitoring, constitute a viable path also in the field of AI-driven health insurance, taking into account the additional impact that such contracts may have on the fundamental right to self-determination in healthcare. Nevertheless, informed consent as a tool for protecting informational self-determination is significantly undermined if we consider that dense information notices are bypassed by consents given for the sole purpose of accessing the service more quickly and if we consider how, even with an awareness of the importance of one's own data, there is a lack of tools to ensure the authenticity of the will expressed.[134]

According to the analysis conducted, HI contracts may respond to current medical poverty and to recent technical developments, but their validity depends on specific structural conditions. Surveillance-enabled features must not eliminate the aleatory element of risk that underpins insurance; parametric instruments must protect the indemnity principle and must not be repurposed into index-based products; parametric coverage must not prevent a static reconstruction of the original risk profile; the continuous surveillance-driven contract could broaden the insurance coverage, especially where the National system does not allow for immediate and effective care; the Premium narrative[135] linked to these products cannot lead to terminate the contract whenever the policyholder does not want to be monitored, since a standard base contract should always be available, except for legally non-insurable risks.

[133] S Thobani, 'Processing Personal Data and the Role of Consent' (2020) EJPLT 93-104.
[134] On the consent dilemma, see S Thobani, 'Il consenso nella regolazione sulla circolazione dei dati' (2025) in Pers. merc. 473.
[135] A Troiano, 'Wearables and Personal Health Data' (2017) 82 Brook. L. Rev. 1750-1751.

Sabro E, Torralbo Muñoz B, 'Redefining "reasonable harm" to privacy in the digital surveillance era: a critical analysis of israeli legal framework' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252SETMB

EJPLT
ISSN 2704-8012

Redefining "reasonable harm" to privacy in the digital surveillance era: a critical analysis of israeli legal framework

Ridefinire il 'danno ragionevole' alla privacy nell'era della sorveglianza digitale: un'analisi critica del quadro giuridico israeliano

EYAL SABRO
Lawyer, Privacy consultant & DPO
University of Cordoba

BARTOLOMÉ TORRALBO MUÑOZ
Assistant Professor, Ph.D. in Criminal Law
University of Cordoba

Abstract

This article examines the concept of "reasonable harm" to privacy in the context of digital surveillance, focusing on Israel's legal framework. It analyzes tensions between formal legal definitions and public perceptions of privacy violations, revealing significant gaps that complicate the establishment of coherent standards. The Israeli case demonstrates how traditional spatial conceptions of privacy are increasingly inadequate in digital environments where information flows transcend physical boundaries. Empirical research highlights the "privacy paradox" in Israeli society – the discrepancy between expressed privacy concerns and actual privacy-protective behaviors. The article proposes new legal tests for evaluating privacy violations that incorporate considerations of chilling effects, contextual integrity, proportionality, and procedural safeguards. By developing more nuanced approaches to these questions, democracies can work toward a future where security and privacy are recognized as complementary rather than competing values.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Questo articolo esamina il concetto di "danno ragionevole" alla privacy nel contesto della sorveglianza digitale, concentrandosi sul quadro giuridico israeliano. Analizza le tensioni tra definizioni legali formali e percezioni pubbliche delle violazioni della privacy, rivelando lacune significative che complicano la definizione di standard coerenti. Il caso israeliano dimostra come le concezioni spaziali tradizionali della privacy siano sempre più inadeguate negli ambienti digitali dove i flussi di informazioni trascendono i confini fisici. La ricerca empirica evidenzia il "paradosso della privacy" nella società israeliana – la discrepanza tra preoccupazioni espresse sulla privacy e comportamenti effettivi di protezione. L'articolo propone nuovi test legali per valutare le violazioni della privacy che incorporano considerazioni sugli effetti inibitori, l'integrità contestuale, la proporzionalità e le salvaguardie procedurali. Sviluppando approcci più sfumati a queste questioni, le democrazie possono lavorare verso un futuro in cui sicurezza e privacy sono riconosciute come valori complementari piuttosto che competitivi.

Keywords: privacy; digital surveillance; reasonable harm; Israeli law; proportionality; contextual integrity

Summary: 1. Introduction: The Dialectic of Privacy and Security in Modern Surveillance. – 2. Theoretical Framework: Evolving Privacy Conceptions in a Digital Landscape. – 2.1. The Epistemological Crisis of "Reasonable Harm" in the Digital Surveillance Era. – 2.2. From Spatial to Contextual Understanding of Privacy. – 2.3. Privacy and Security in Democratic Societies. – 2.4. The Chilling Effect and Democratic Participation. – 3. The Israeli Legal Framework for Digital Privacy and Surveillance. – 3.1. Constitutional Protection of Privacy. – 3.2. The Privacy Protection Law and Its Implementation. – 3.3. Wiretapping and Communications Data Laws. – 3.4. Recent Legislative Developments: The Spyware Law. – 3.5. Judicial Interpretation of Privacy in Surveillance Contexts. – 3.6. The Constitutional Paradox: Fundamental Rights with Structural Immunity. – 4. The Gap Between Legal Definitions and Public Perceptions. – 4.1. Empirical Evidence of Public Privacy Concerns. – 4.2. The Privacy Paradox in Israeli Society. – 4.3. The Enforcement Gap. – 4.3.1 Case Study: The Enforcement Gap as Epistemic Crisis. – 5. Developing New Legal Tests for "Reasonable Harm". – 5.1 The Chilling Effect Test. – 5.2. The Contextual Integrity Framework. – 5.3 The Proportionality Requirement. – 5.4 The Independent Oversight Mechanisms. – 6. Conclusion: Reimagining Privacy Protections in an Era of Pervasive Surveillance.

1. Introduction: The Dialectic of Privacy and Security in Modern Surveillance.

The fundamental question of what constitutes "reasonable harm" to privacy in an era of pervasive digital surveillance has emerged as one of the most challenging legal dilemmas faced by modern democracies. As digital technologies increasingly permeate daily life, the capacity for surveillance by state entities and private actors alike has expanded exponentially, creating unprecedented tensions between security imperatives and privacy rights. This

dialectic is particularly pronounced in Israel, where a unique confluence of security concerns, democratic values, and rapid technological innovation has created a complex legal landscape for privacy protection.

The core research question this article addresses is how to define "reasonable harm" to privacy from a legal perspective in an era of extensive digital surveillance. Specifically, what tensions exist between formal legal definitions of harm and public perceptions of privacy violations? How have Israeli courts interpreted this concept, and what new legal tests might better balance the competing interests at stake?

Israel presents a particularly compelling case study for examining these questions. As a democracy facing persistent security challenges, Israel has developed sophisticated surveillance capabilities while maintaining a commitment to democratic principles and the protection of fundamental rights. This tension has led to a distinctive body of case law and legislation that reflects broader global challenges in reconciling privacy and security interests. The Israeli Basic Law: Human Dignity and Liberty (1992) provides constitutional protection for privacy, yet security exceptions and expansive surveillance authorities create a complex regulatory environment.

The relevance of this inquiry extends beyond Israeli borders. As Heikkilä argues, "the challenge of reconciling surveillance imperatives with privacy protection is fundamental to modern democratic governance worldwide".[1] This challenge has only intensified following Edward Snowden's revelations about mass surveillance programs, which sparked global debates about the permissible boundaries of state monitoring.[2]

By exploring these questions, this article contributes to both scholarly debates and practical policy discussions about privacy protection in the digital age. It argues that traditional conceptions of privacy harm are inadequate for addressing the novel challenges posed by modern surveillance technologies, and that new frameworks incorporating elements of contextual integrity, proportionality, and transparent oversight are needed to ensure meaningful privacy protection while accommodating legitimate security interests.

2. Theoretical Framework: Evolving Privacy Conceptions in a Digital Landscape.

2.1 The Epistemological Crisis of "Reasonable Harm" in the Digital Surveillance Era.

In contemporary privacy law, the dominant harm-based approach typically requires that claimants demonstrate a cognizable, "reasonable" or "reasonably foreseeable" harm as a precondition for legal intervention. Under this standard, courts and regulators are expected to translate diffuse privacy concerns into concrete, individualized injuries that can be recognised,

[1] H Heikkilä, 'Beyond Moral Coupling: Analysing Politics of Privacy in the Era of Surveillance' (2020) 8 Media and Communication 248, 250.
[2] N Ni Loideain, 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era' (2015) 3 Media and Communication 53, 54.

measured, and remedied on a case-by-case basis, while filtering out speculative, abstract, or purely dignitary interests.[3]

Against this background, before delving deeper into evolving privacy conceptions, we must confront a fundamental conceptual crisis: the very definition of “reasonable harm” as an appropriate legal framework for evaluating privacy violations in the digital age.

The problem is not merely practical, that is, difficulties in measuring or quantifying intangible harms, but substantive: the harm paradigm relies on a dichotomy between a normative baseline state and a measurable deviation from it. As Solove and Citron demonstrate, legal doctrines built around concrete, individualized injury struggle to accommodate the diffuse, cumulative, and often intangible nature of contemporary privacy harms.[4] However, in the context of digital surveillance, the very architecture of monitoring and collection creates a new reality of "surveillance normalization”[5] in which the concept of "harm" as a deviation from a norm becomes incoherent.[6] As evident from an examination of Israeli jurisprudence, courts are forced to retroactively invent indicators for "harm" that were not theoretically developed in the first place, thereby producing a legal fiction that masks the concept's inadequacy to technological reality. In practice, the reasonable harm threshold enables courts and regulators to translate diffuse privacy concerns into discrete, litigable injuries that can be recognized, measured, and remedied on a case-by-case basis.

The legal fiction of "reasonable harm" allows courts to adjudicate concrete cases while creating an illusion of doctrinal continuity. Still, it conceals the deeper failure: our inability to conceptualize privacy infringement in the digital surveillance era in terms of singular, measurable, and immediate "harm." The fundamental question, then, is not merely what constitutes "reasonable harm," but whether the very use of the harm paradigm remains effective or has become anachronistic in an era where the potential for privacy violations is structural, persistent, and often invisible. As Parsons argues, pervasive mass surveillance erodes the communicative conditions of democracy itself, producing harms that are structural and societal rather than discrete and individualized.[7]

---

[3] DJ Solove, DK Citron, ‘Privacy Harms’ (2022) 102 Boston University Law Review 793; Office of Information Policy, ‘OIP Guidance: Applying a Presumption of Openness and the Foreseeable Harm Standard’ (US Department of Justice, 3 September 2024); ‘Foreseeable Harm Standard’ (FOIA Wiki, 2025).

[4] See ibid (2022) 102 Boston University Law Review 793.

[5] LK Donohue, ‘Surveillance Normalization’ (2023) *Harvard Civil Rights-Civil Liberties Law Review* (forthcoming). See also D Mac Síthigh and A Murschetz, ‘The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates after the Snowden Revelations’ (2017) International Journal of Communication 11.

[6] E Selinger, JH Rhee, ‘Normalizing Surveillance’ (2021) 22(1) Nordic Journal of Applied Ethics 49.

[7] C Parsons, ‘Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance’ (2015) 3 Media and Communication 1.

2.2 From Spatial to Contextual Understanding of Privacy.

The inadequacy of spatial metaphors for understanding privacy in digital contexts has led scholars to develop more nuanced theoretical frameworks. Nissenbaum's theory of contextual integrity offers a particularly valuable approach, suggesting that privacy violations occur not simply when information moves from a "private" to a "public" sphere, but when information flows transgresses contextual norms governing the appropriate collection, use, and dissemination of information.[8]

In the Israeli context, this evolution from spatial to contextual understanding of privacy is evident in case law. In Ploni v The Regional Rabbinical Court in Netanya (HCJ 6650/04), the Supreme Court recognized that privacy rights can exist even in shared spaces, holding that filming a spouse in their shared home without consent constitutes a privacy violation. The Court emphasised that the decisive question is not the formal status of the space (private or shared), but the nature of the relationship between the parties and the reasonable expectations of privacy that arise within it, particularly in intimate and vulnerable settings such as the home. In doing so, the Court signaled a move away from a rigid spatial conception of privacy toward a contextual approach that evaluates how surveillance practices disrupt trust, autonomy, and legitimate expectations within specific social relationships.

This represents a significant shift from purely spatial conceptions of privacy toward a more contextual understanding that considers relationship dynamics and reasonable expectations in a specific situation.[9]

2.3 Privacy and Security in Democratic Societies.

The theoretical foundation for balancing privacy and security interests in democratic societies typically draws on principles of proportionality, necessity, and transparent oversight. The proportionality principle, which features prominently in Israeli constitutional jurisprudence, requires that any infringement of fundamental rights be proportionate to the legitimate aim pursued. As Barak has shown, proportionality in the Israeli context is structured as a four-stage test, requiring a proper purpose, a rational connection between means and end, use of the least restrictive means, and a final balancing between the benefit of the measure and the harm to the right.[10]

This principle provides a framework for assessing whether surveillance measures that impinge on privacy constitute "reasonable harm" or cross the threshold into disproportionate violations, as articulated through the three-stage proportionality test developed under the limitations clause of Basic Law: Human Dignity and Liberty.[11]

---

[8] H Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119, 136-38.
[9] HCJ 6650/04 *Ploni v. The Regional Rabbinical Court in Netanya* [2006] unpublished.
[10] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press 2012).
[11] CA 6821/93 United Mizrahi Bank Ltd v Migdal Cooperative Village IsrSC 49(4) 221; see also 'Israel's Basic Law on Human Dignity and Liberty, 1992' (Palestine Open Maps, 2011) (describing the limitations clause as a proportionality test composed of rational connection, least restrictive means and balancing).

2.4 The Chilling Effect and Democratic Participation.

A crucial theoretical dimension of privacy harm in surveillance contexts concerns what has been termed the "chilling effect," the tendency for surveillance to inhibit lawful activities, free expression, and democratic participation. As Zuboff argues, surveillance can fundamentally alter behavior and undermine autonomy, even without direct coercion. This dimension of harm extends beyond individual privacy violations to implicate broader democratic values.[12]

In that matter, at the beginning of the 20th century, Richards already contended that surveillance itself must be recognised as a constitutional harm, given its chilling effects on intellectual privacy and its distortion of power relations between watcher and watched, even in the absence of demonstrable, event-like injury.[13]

Research in Israel has empirically demonstrated this effect. A 2020 study by the Heinrich Böll Foundation found that awareness of governmental surveillance led to behavioural modifications among Israeli citizens, with 41% of Arabic-speaking respondents and 29% of Hebrew-speaking respondents expressing concerns about digital monitoring.[14]

3. The Israeli Legal Framework for Digital Privacy and Surveillance.

3.1 Constitutional Protection of Privacy.

Unlike many Western democracies, Israel lacks a formal written constitution. Instead, a series of Basic Laws serves as the constitutional cornerstone, with the Basic Law: Human Dignity and Liberty (1992) providing the constitutional foundation for privacy protection. Article 7 of this Basic Law states, "All persons have the right to privacy and intimacy," and specifically prohibits searches of a person's private premises, body, or possessions, as well as the violation of a person's privacy in conversations, writings, or records.[15]

Privacy enjoys a privileged status in Israel's constitutional hierarchy as one of the few rights explicitly enumerated in the Basic Law. However, like other constitutional rights in Israel, privacy protection is not absolute. Article 8 of the Basic Law establishes that rights may be infringed by laws "befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required". [16] This proportionality clause provides the constitutional foundation for balancing privacy against competing interests, particularly security concerns. This requirement is anchored in the "limitations clause" of

---

[12] Zuboff shows how surveillance capitalism shifts from merely predicting behaviour to systematically modifying it, thereby eroding individual autonomy even in the absence of overt coercion. See S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

[13] NM Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934.

[14] Heinrich Böll Foundation, 'Invisible Surveillance, Indifferent Publics: Israeli Perceptions of Surveillance (2020) <https://il.boell.org/sites/default/files/2020-11/Invisible-Surveillance-Indifferent-Publics-Israeli-Perceptions.pdf> accessed 20 March 2023.

[15] Basic Law: Human Dignity and Liberty, 5752-1992, SH No. 1391, 150, art 7.

[16] ibid art 8.

Basic Law: Human Dignity and Liberty, which permits infringements of constitutional rights only when they serve a proper purpose and are limited "to an extent no greater than is required".[17]

3.2 The Privacy Protection Law and Its Implementation.

The Privacy Protection Law (1981) predates the Basic Law but serves as the primary legislative framework governing privacy in Israel. Section 2 of the Law defines privacy violations to include various forms of surveillance, such as "spying on or trailing a person in a manner likely to harass them, or any other harassment," as well as "photographing a person while they are in a private domain," and "the violation of the duty of confidentiality prescribed by law regarding a person's private affairs".[18]

Notably, the Privacy Protection Law includes exemptions for security authorities under Section 19(b), which states that "a security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for performance thereof". This provision effectively grants security authorities broad immunity from civil liability under the Privacy Protection Law for surveillance activities carried out within the scope of their official duties, so long as those activities can be justified as "reasonably" connected to their mandated functions.[19]

Empirical analysis of judicial decisions under the Privacy Protection Law reveals interesting patterns in its implementation. A study examining a decade of Israeli judicial decisions on data protection (2012-2022) found that civil lawsuits for privacy violations constitute a negligible share of all civil proceedings in Israel.[20] The most common ground for civil lawsuits under the Privacy Protection Law is "spying on or tracing a person", which appears in 36.9% of civil court rulings.[21] However, claims related to privacy violations in databases, a critical area in the context of digital surveillance, were virtually non-existent in civil lawsuits, suggesting potential gaps in enforcement or public awareness.

3.3 Wiretapping and Communications Data Laws.

Israel's legal framework for communications surveillance is primarily governed by two key laws: the Wiretap Law (1979) and the Communications Data Law (2007). These laws establish the conditions under which state authorities may intercept communications or access communications metadata.

The Wiretap Law permits wiretapping for national security purposes with ministerial authorization, while law enforcement wiretapping requires judicial

[17] Basic Law: Human Dignity and Liberty 5752-1992, s 8.
[18] Privacy Protection Law, 5741-1981, SH No. 1011, 128, s 2.
[19] ibid s 19(b).
[20] R Dvash, 'Analysis of a Decade of Israeli Judicial Decisions Related to Data Protection (2012-2022)' (Future of Privacy Forum, 27 April 2023) <https://fpf.org/blog/analysis-of-a-decade-of-israeli-judicial-decisions-related-to-data-protection-2012-2022/> accessed 1 April 2023.
[21] ibid.

approval. Although this dual-track system attempts to balance security needs with privacy protections, critics have noted that it creates significant disparities in oversight. As Cahane observes, "The procedural and substantive safeguards in place for security wiretapping are weaker than those for law enforcement wiretapping, raising concerns about adequate protection against disproportionate surveillance".[22]

The Communications Data Law authorizes law enforcement agencies to obtain communications metadata from service providers for investigation, detection, and prevention of crime. The law requires judicial approval for metadata requests, except in urgent cases. However, it does not apply similar restrictions to intelligence agencies accessing the same data. This discrepancy in treatment has been criticized as creating a significant loophole in privacy protection.

3.4 Recent Legislative Developments: The Spyware Law.

In November 2024, the Israeli Knesset preliminarily approved the controversial Bill on Police Access to Computer Material (commonly referred to as the "Spyware Law"),[23] which would grant the police expanded surveillance powers.[1] The proposed law would authorize the use of court-approved surveillance technology for serious offenses punishable by ten years or more in prison, where covert searches are crucial to investigating and preventing criminal acts effectively.[24]

The Spyware Law has faced significant criticism from both the Public Defender's Office and the Attorney General, who argue that it represents "a severe blow to the rule of law" and would create a "severe violation of the constitutional right to privacy". [25] Particularly controversial is the law's exclusion of public corruption offenses from its scope, which critics argue could shield government officials from accountability.

3.5 Judicial Interpretation of Privacy in Surveillance Contexts.

Israeli courts have developed a significant body of case law interpreting privacy rights in the context of surveillance. A key concept that has emerged is the "reasonable expectation of privacy" test, which evaluates whether an individual can reasonably expect privacy in a specific situation. This test was articulated in Ploni v The Regional Rabbinical Court in Netanya (HCJ 6650/04), where the Supreme Court held that filming a spouse in their shared home without consent constitutes a privacy violation, even though the space was shared.[1] The Court stressed that the existence of privacy does not depend

[22] A Cahane, 'Regulation of Online Surveillance in Israeli Law and Comparative Law' (Israel Democracy Institute, January 2019) 233.
[23] See eg, P Cohen, 'Israeli Government Advances "Spyware Law" Without Anti-Bribery Clause' (1 December 2024) <https://www.pearlcohen.com/israeli-government-advances-spyware-law-without-anti-bribery-clause/> (linking to the full text of the Bill on Police Access to Computer Material in Hebrew). Also see T Hilaie, 'The "Spyware Law" Passed Preliminary Approval, The Opposition Boycotted' (13 November 2024).
[24] T Hilaie, 'The "Spyware Law" Passed Preliminary Approval, The Opposition Boycotted' (13 November 2024).
[25] T Zimuki, 'The Attorney General Opposes a Law Advanced by the Coalition: Demands Spyware Use Also in Cases of Government Corruption' (31 October 2024).

solely on the formal classification of a space as “private” or “public”, but on the nature of the relationship and the legitimate expectations of privacy that arise within it, particularly in intimate settings such as the home.[26]

In Fisher v. State of Israel (2021), the National Labor Court established important precedents regarding workplace surveillance, ruling that employers must obtain explicit written consent for monitoring employees' emails or digital activities and must minimize privacy infringements to the absolute minimum necessary.[27] This decision reflects a growing judicial recognition of the need for explicit consent and proportionality in digital surveillance contexts.

The courts have also addressed the use of advanced surveillance technologies. In Orich v. State of Israel (2023), the court established a precedent that searching mobile devices without a detailed judicial warrant constitutes a disproportionate invasion of privacy, calling for legislative updates to regulate the use of advanced surveillance technologies.[28]

3.6 The Constitutional Paradox: Fundamental Rights with Structural Immunity.

A deeper analysis of the Israeli legal system reveals a substantive paradox that undermines privacy protection: on one hand, the Basic Law: Human Dignity and Liberty provides constitutional protection for privacy, while on the other hand, Section 19(b) of the Privacy Protection Law grants broad exemptions to security authorities acting "within the scope of their functions”. This paradox raises a penetrating question: can privacy be genuinely considered a fundamental right when the entities with the most tremendous potential to infringe upon it enjoy structural immunity? This contradiction becomes more acute in light of statistics showing that 99.3% of wiretap requests were approved in 2021. This figure suggests that judicial review, which should ensure proportionality, has become an almost automatic approval mechanism, effectively emptying procedural protections of substantive content. This situation compels us to question whether the constitutional doctrine of proportionality, which the court relies upon so heavily, has become a mere rhetorical device that legitimizes rather than constrains state surveillance.

The structural contradictions within the Israeli legal framework exemplify what legal philosopher Gunther Teubner identifies as "constitutional moments": instances in which the internal logic of a legal system confronts its limitations. [29] In the case of privacy protection, the Israeli legal system simultaneously affirms privacy as a constitutional right while systematically undermining its enforceability against the state's most powerful surveillance actors. This is not merely a technical inconsistency but reveals a more profound epistemic crisis in privacy law's ability to conceptualize harm in the surveillance context.

---

[26] HCJ 6650/04 Ploni v The Regional Rabbinical Court in Netanya (unpublished).
[27] National Labor Court Case 90/08 *Isakov v. State of Israel* [2021].
[28] *Orich v. State of Israel [2023].*
[29] G Teubner, ‘A Constitutional Moment? The Logics of “Hitting the Bottom”’ in PF Kjaer, G Teubner and A Febbrajo (eds.) *The Financial Crisis in Constitutional Perspective: The Dark Side of Functional Differentiation* (Hart Publishing 2011).

4. The Gap Between Legal Definitions and Public Perceptions.

A critical dimension in analyzing what constitutes "reasonable harm" to privacy is understanding the gap between formal legal definitions and how the public perceives and experiences privacy violations.

4.1 Empirical Evidence of Public Privacy Concerns.

Empirical research on privacy perceptions in Israel reveals complex and sometimes contradictory public attitudes. A 2020 study by the Heinrich Böll Foundation found significant levels of unawareness and indifference regarding state surveillance programs: 41% of Arabic-speaking respondents and 29% of Hebrew-speaking respondents were unaware of mass surveillance of cellular data for COVID-19 contact tracing, while 54% of Jewish respondents and 65% of Arab respondents expressed indifference or hesitation about the surveillance's implications for their privacy.[30]

This relative indifference contrasts with heightened concerns in specific contexts. Research on social media privacy in Israel has found that, despite awareness of privacy risks, 82% of Israeli users continue to share personal information online, exhibiting what researchers term "selective awareness," recognizing privacy risks while believing they primarily affect others rather than themselves.[31] This disconnect between abstract privacy concerns and actual behavior creates significant challenges for determining what constitutes "reasonable" privacy expectations in legal contexts.

4.2 The Privacy Paradox in Israeli Society.

The discrepancy between expressed privacy concerns and actual privacy-protective behaviors, often referred to as the "privacy paradox," is particularly pronounced in Israeli society. The discrepancy between expressed privacy concerns and actual privacy-protective behaviors, often referred to as the “privacy paradox”, is particularly pronounced in Israeli society.[32]

Annual surveys by the Israel Democracy Institute (2015-2017) revealed that 68% of Israelis are willing to sacrifice privacy for improved personal security.[33] At the same time, 57% expressed concerns about the potential misuse of biometric data by authorities, despite a majority supporting the implementation of biometric technologies for security purposes.[34]

---

[30] Heinrich Böll Foundation, 'Invisible Surveillance, Indifferent Publics: Israeli Perceptions of Surveillance' (2020) <https://il.boell.org/sites/default/files/2020-11/Invisible-Surveillance-Indifferent-Publics-Israeli-Perceptions.pdf> accessed 20 March 2023.

[31] 'Privacy in New Media in Israel: How Social Networks are Helping to Shape the Perception of Privacy in Israeli Society' (2018) 17 Journal of Media Studies 203, 211-15.

[32] Y Karniel and A Lavie-Dinur, ‘Privacy in New Media in Israel: How Social Networks Are Helping to Shape the Perception of Privacy in Israeli Society’ (2018) 17 Journal of Media Studies 203 (identifying a marked gap between Israeli users’ awareness of online privacy risks and their continued willingness to share personal information online); Israel Democracy Institute, ‘Privacy in a Digital World’ (2019) <https://en.idi.org.il/articles/28743> (describing the “privacy paradox” as a central feature of Israelis’ digital behaviour).

[33] Israel Democracy Institute, 'The Israeli Democracy Index (2017)' <https://en.idi.org.il/publications/6688> accessed 25 March 2023.

[34] ibid.

This paradox reflects broader cultural and social factors specific to the Israeli context. As one study notes, "The collectivist nature of Israeli society encourages information sharing as part of community identity, even at the expense of privacy [35]".This cultural tendency, combined with the heightened security concerns that characterize Israeli society, creates a distinctive context for privacy perceptions that differs from other democratic institutions.

4.3 The Enforcement Gap.

4.3.1 Case Study: The Enforcement Gap as Epistemic Crisis.

The stark empirical data concerning privacy enforcement reveal more than mere procedural failures; they illuminate a fundamental epistemic crisis in privacy law. The Future of Privacy Forum's study, which found that only 12% of civil claims under the Privacy Protection Law were successful, represents not simply an enforcement gap but a systemic failure to recognize privacy harms as legally cognizable injuries. This crisis is particularly evident in cases involving database violations, which are virtually absent from civil litigation despite their central role in digital surveillance. This absence reflects the law's conceptual blindness to forms of privacy harm that do not manifest as immediate, individualized, and tangible injuries. When privacy violations occur through data processing, which is often invisible, cumulative, and delayed in its effects, the traditional harm-based legal framework fails to provide meaningful recognition or redress.

The data showing that privacy-related class actions represent only 4.5% of all class actions in Israel further demonstrates this epistemic failure. Class actions theoretically provide a mechanism for addressing collective harms that might be individually diffuse. Yet their underutilization in privacy contexts suggests that even collective legal mechanisms remain trapped within an individualistic harm paradigm that cannot adequately conceptualize privacy violations as structural or societal harms. This case study illustrates the broader theoretical problem identified earlier: the legal system continues to rely on observable, measurable "harms" as triggers for legal intervention, even as the most serious surveillance harms have become normalized, invisible, or deferred. The enforcement gap is thus not merely a practical problem of insufficient litigation or legal barriers, but a manifestation of the fundamental inadequacy of harm-based privacy frameworks in the surveillance age.

5. Developing New Legal Tests for "Reasonable Harm".

The preceding analysis demonstrates the inadequacy of current approaches to defining "reasonable harm" to privacy in digital surveillance contexts. This section proposes new legal tests to provide more nuanced, context-sensitive approaches to evaluating privacy violations in the digital age.

[35] 'Privacy in New Media in Israel: How Social Networks are Helping to Shape the Perception of Privacy in Israeli Society' (2018) 17 Journal of Media Studies 203, 220.

5.1 The Chilling Effect Test.

A crucial dimension of privacy harm that is often overlooked in traditional legal frameworks is the "chilling effect" that surveillance can have on protected activities and democratic participation. A new legal test for reasonable harm should explicitly incorporate assessment of these chilling effects, recognizing that privacy violations can cause harm beyond direct informational disclosures.

Under this proposed test, courts would evaluate:

1. Whether the surveillance measure in question has a demonstrable or likely effect on lawful behavior, including political expression, association, or other constitutionally protected activities.
2. The extent to which individuals are aware of the surveillance measure and might reasonably modify their behavior in response.
3. Whether particular groups or communities are disproportionately affected by potential chilling effects, especially those that have historically been subject to heightened monitoring.

5.2 The Contextual Integrity Framework.

Drawing on Nissenbaum's theory of contextual integrity, this proposed test would assess privacy violations by whether they transgress contextual informational norms rather than by absolute public-private distinctions. This approach is particularly well-suited to addressing privacy in networked digital environments.

Under this test, courts would evaluate:

1. The context in which information was shared or collected, including the relationships between parties and the purpose of sharing;
2. Whether the subsequent use, processing, or dissemination of the information violated reasonable expectations within that context;
3. Whether the information flow transgressed established norms for similar contexts in ways that individuals could not reasonably anticipate.

This test finds support in emerging Israeli case law, particularly in decisions such as Ploni v. The Regional Rabbinical Court in Netanya (HCJ 6650/04) and Jarais v. State of Israel (Criminal Appeal 2126/05), which have begun to move away from strict spatial definitions of privacy toward more contextual understandings.[36] It would provide a more flexible framework for addressing privacy violations in digital contexts where traditional boundaries between public and private spaces are increasingly blurred.

5.3 The Proportionality Requirement.

Drawing on Israel's constitutional proportionality test, this proposed approach would incorporate a structured proportionality analysis tailored explicitly to surveillance contexts. While proportionality principles are already applied in some privacy cases, a more structured framework would provide greater consistency and clarity.

Under this test, courts would systematically evaluate:

[36] HCJ 6650/04 *Ploni v The Regional Rabbinical Court in Netanya* (unpublished).

1. Whether the surveillance measure serves a legitimate aim;
2. Whether the measure is suitable for achieving that aim;
3. Whether the measure is necessary, in the sense that no less privacy-invasive alternative would achieve the same aim;
4. Whether the measure is proportionate in the narrow sense, meaning that the importance of the aim justifies the extent of the privacy infringement.

This structured approach would require authorities to demonstrate not only that surveillance measures serve legitimate security or law enforcement purposes, but also that they represent the least invasive means of achieving those purposes. It would provide a more rigorous framework for assessing the reasonableness of privacy infringements in security contexts.

5.4 The Independent Oversight Mechanisms.

A final proposed test focuses not on the nature of the surveillance itself but on the procedural safeguards surrounding it. This test recognizes that the reasonableness of privacy infringements depends not only on their substantive characteristics but also on the oversight mechanisms that prevent abuse.

Under this test, courts would evaluate:

1. Whether prior independent authorization was required and obtained for the surveillance measure.
2. Whether ongoing independent oversight exists to monitor implementation and prevent scope creep.
3. Whether affected individuals have meaningful opportunities for ex post review and redress.

This test addresses concerns raised by empirical evidence showing that nearly 100% of surveillance requests are approved in Israel, with 99.3% of wiretap requests approved in 2021. It recognizes that effective oversight[37] is essential for ensuring that surveillance remains within reasonable bounds and does not result in disproportionate privacy violations.

6. Conclusion: Reimagining Privacy Protections in an Era of Pervasive Surveillance.

This article has examined the complex challenge of defining "reasonable harm" to privacy in the context of digital surveillance, with a particular focus on the Israeli legal framework. Through analysis of theoretical approaches, empirical evidence, and legal developments, it has identified significant gaps between formal legal definitions and public perceptions of privacy violations. These gaps complicate efforts to establish coherent standards for evaluating when surveillance activities cross the threshold from legitimate security measures to disproportionate intrusions on privacy.

The analysis highlights several key findings with broader implications for privacy protection in democratic societies. First, traditional spatial conceptions

[37] A Viner and H Tamam Ben-Avraham, 'Intrusion and Search Technologies in Smart Devices and Digital Assets Employed by Law Enforcement Authorities in Israel' (January 2023) 35.

of privacy centered on distinctions between "public" and "private" spaces are increasingly inadequate in digital contexts where information flows transcend physical boundaries. Israeli courts have begun to recognize this inadequacy; however, statutory frameworks have not yet fully incorporated this evolving understanding.

Second, empirical research reveals significant disparities between expressed privacy concerns and actual privacy-protective behaviors among Israeli citizens, a manifestation of the "privacy paradox" observed in other contexts. These disparities are shaped by cultural, social, and historical factors specific to the Israeli context, including the collectivist nature of Israeli society and heightened security concerns. They complicate efforts to establish objective standards for "reasonable" privacy expectations and highlight the need for context-sensitive approaches.

Third, the current legal framework governing surveillance in Israel contains significant gaps and inconsistencies. The dual-track system for authorizing surveillance, with weaker protections for security-related monitoring compared to law enforcement activities, creates disparities in oversight. High approval rates for surveillance requests raise questions about the effectiveness of judicial authorization as a safeguard against disproportionate privacy violations.

Based on these findings, the article has proposed new legal tests for evaluating "reasonable harm" to privacy in surveillance contexts. These tests incorporate considerations of chilling effects on protected activities, contextual informational norms, structured proportionality analysis, and procedural safeguards. Together, they provide a more comprehensive framework for assessing privacy violations that accounts for both direct and indirect effects, individual and societal impacts, and substantive and procedural dimensions of privacy protection.

The path forward requires not merely incremental legal reforms but a paradigmatic shift in how we conceptualize privacy and its relationship to surveillance in democratic societies. This article argues that the legal system must abandon harm-based thresholds altogether in surveillance law. The traditional requirement to demonstrate "reasonable harm" as a prerequisite for legal intervention has proven fundamentally inadequate in addressing the structural, cumulative, and often invisible nature of privacy violations in the digital surveillance era. Instead, the article proposes a radical inversion of the current framework: a presumption of harm should attach to all unconsented data collection by state actors. This presumption would shift the burden of justification to the surveillance authority, requiring it to demonstrate not merely that the harm is "reasonable", but that the surveillance activity serves a compelling interest that cannot be achieved through less intrusive means. Such a shift would recognize that in an era of pervasive surveillance capabilities, privacy protection requires proactive safeguards rather than reactive remedies for demonstrable harms. Moreover, the legal system must reconceptualize privacy not merely as an individual right but as a structural precondition for democratic participation. The current individualistic focus of privacy law fails to account for the collective dimensions of surveillance, including how it shapes

public discourse, chills political expression, and reinforces existing power asymmetries.

By recognizing privacy as a public good essential to democratic functioning, rather than merely a personal preference subject to individual trade-offs, the legal system can develop more robust protections against surveillance excesses. The Israeli experience with its distinctive combination of security challenges, democratic values, and technological innovation offers valuable insights for this necessary reconceptualization of privacy protection. By confronting the fundamental contradictions in its legal framework and developing new approaches that move beyond harm-based paradigms, Israel can pioneer a more effective model for protecting privacy in the surveillance age. Such innovation is urgently needed not only in Israel but in democracies worldwide grappling with similar tensions between security imperatives and fundamental rights.

Senatore A, 'Analisi della comunicazione pubblicitaria: mercato e diritti fondamentali' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252AS

EJPLT
ISSN 2704-8012



Analisi della comunicazione pubblicitaria: mercato e diritti fondamentali

Analysis of advertising communication: market and fundamental rights

ANDREA SENATORE
Assegnista di ricerca post-doc
Università degli Studi di Salerno

Abstract

Il contributo si propone di analizzare alcuni aspetti della comunicazione pubblicitaria. A fronte di un mercato sempre in espansione, in grado di superare le tradizionali unità di tempo, spazio e luogo, la tematica non riguarda soltanto la tutela del mercato bensì i principi giuridici di questo e il ruolo assiologico del consumatore-persona. Tuttavia la comunicazione del messaggio non è solamente circoscritta alla pubblicità commerciale, rilevando anche come modalità di trasmissione di pensieri e opinioni che abbracciano ambiti non solo legati al consumo.

This work aims to analyze some aspects of advertising. In the face of an ever-expanding market, able to overcome the traditional unities of time, space and place, the issue does not affect market protection only but rather the legal principles of this and the axiological role of the consumer-person. However, communication of messages is not only limited to commercial advertising, but also plays a role as a way of transmitting thoughts and opinions that embrace areas not only consumer-related.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: pubblicità; pubblicità commerciale; consumatori; minore consumatore; manifestazione del pensiero; pubblicità ideologica

Summary: 1. Introduzione: evoluzione della pubblicità commerciale e dei consumatori. – 2. Caratteri della pubblicità commerciale nel prisma della rilevanza costituzionale del mercato. – 3. Il sistema rimediale. – 4. Pubblicità (anche) come *medium* di manifestazione del pensiero. – 5. Osservazioni conclusive.

1. Introduzione: evoluzione della pubblicità commerciale e dei consumatori.

Già da tempo la dottrina registra il passaggio della pubblicità commerciale dalla mera funzione di strumento informativo delle caratteristiche di un determinato prodotto ad una di persuasione morale, che oramai ha assunto dei tratti prevalenti[1]. Si tratta, tuttavia, di un fenomeno che ha origini antiche, direttamente collegabili allo sviluppo delle prime attività commerciali e dalle relative iscrizioni, insegne[2] o simboli merceologici per fini propagandistici e di

[1] Cfr. S. GATTI, *Pubblicità commerciale*, in *Enc. dir.*, XXXVI, Milano, 1988, 1058.

[2] È appena il caso di ricordare che l'insegna ha la funzione di individuare il luogo ove si svolge l'attività d'impresa, sia di produzione sia, ad es., di vendita al dettaglio ed ha una precisa funzione distintiva (cfr. art. 2568 c.c.) che rende immediatamente distinguibile un'azienda da un'altra (cfr. anche art. 2564, 1° co., c.c.). In giurisprudenza v. la risalente ma chiara Cass., 23.04.1966, n. 1042, in *Foro it.*, 1967, I, 90 ss., così massimata: «l'insegna è il segno, nominativo o emblematico, distintivo di un determinato locale nel quale si esercita un'attività imprenditoriale: essa contraddistingue lo stabilimento di un'azienda ed acquista particolare importanza nelle imprese in cui lo stabilimento costituisce il punto di incontro tra imprenditore e clienti e, quindi, il luogo di conclusione degli affari. Dalla funzione dell'insegna di identificare uno stabilimento, commerciale o industriale, consegue il suo collegamento con un'attività imprenditoriale e la sua distinzione dal nome che ha la funzione individuatrice della persona dell'imprenditore e dalla denominazione con la quale l'immobile, come tale, sia individuato. Pertanto, se ad uno stabilimento commerciale o industriale sia attribuita come insegna la denominazione dell'immobile in cui è installato, e successivamente detto stabilimento viene trasferito in altro immobile, legittimamente l'imprenditore può continuare ad usare la precedente insegna». Per il divieto di confusione, v. Cass., 17.01.2017, n. 971, in *www.altalex.com*, con nota di CASABURI, *Nel conflitto tra ditte e insegne confondibili prevale quella usata per prima*, a mente della quale in caso di conflitto tra titolari di insegne uguali o simili per la presenza dello stesso cognome, pur legittimamente usato, «il giudice può disporre modificazioni, aggiunte o soppressioni, fino all'eliminazione del cognome dall'insegna sorta successivamente, ove quel conflitto sia tale da creare confusione per l'oggetto dell'impresa e per il luogo in cui questa è esercitata». Quanto poi all'estensione territoriale, v. Cass., ord. 17.05.2013, n. 12136, in *One LEGALE*, a mente della quale, «il concetto di luogo di esercizio dell'impresa di cui agli artt. 2564 e 2568 c.c., ai fini della tutela in caso di confondibilità fra imprese, non va inteso con esagerato valore restrittivo, dovendosi badare anche agli sviluppi potenziali dell'impresa razionalmente prevedibili, nonché alle pratiche difficoltà, che sovente s'incontrano, ad isolare l'espansione di un'impresa in un determinato ambito territoriale. Pertanto, la localizzazione non deve essere intesa secondo un criterio restrittivo, riguardo soltanto all'attività esplicata in un determinato momento, nel luogo di produzione e di commercio, ma facendo anche riferimento alla possibilità di espansione all'intera zona territorialmente al cosiddetto mercato di sbocco, raggiunta dall'attività complessiva dell'impresa».
Oltre all'insegna sono segni distintivi dell'azienda la ditta e il marchio e, recentemente, il nome a domino ha assunto negli ultimi anni rilevanza, ed anche un notevole valore commerciale, a seguito della diffusione del commercio elettronico e delle piattaforme di vendita online (cfr. art. 23 c.p.i.). La funzione che accomuna i segni distintivi è quella di rendere riconoscibili in un mercato concorrenziale l'imprenditore e i suoi prodotti, di attirare e fidelizzare la clientela, venendo appunto qualificati come «collettori di clientela».
In dottrina, cfr. M. BERTANI, A.E. COGO, P. FABBIO, A. OTTOLIA e A. GENOVESE, *Lineamenti di diritto industriale. Concorrenza e proprietà intellettuale*, Padova-Milano, 2024; A. VANZETTI, V. DI CATALDO e M.S. SPOLIDORO, *Manuale di diritto industriale*, Milano, 2024; B. TASSONE e G. CASSANO, *Diritto industriale e diritto d'autore*

riconoscibilità. La comunicazione pubblicitaria nasce e si sviluppa parallelamente anche alle diverse condizioni sociali, politiche e culturali[3]: si prenda come riferimento la situazione dell'Italia alla fine del XIX secolo[4], ancora prevalentemente ad economia agricola con una situazione di povertà molto diffusa e con enormi differenze socio-economiche tra il Nord e il Sud ed un'alta percentuale di analfabetismo e dove le prime comunicazioni pubblicitarie aumentano con la diffusione dei giornali tra la metà dell'Ottocento e i primi del Novecento[5].

Il settore pubblicitario incide, poi, anche su un'altra materia *id est* il marketing, il modo con cui le imprese – sempre più votate ad una dimensione trans-nazionale – cercano di raggiungere la propria clientela per fidelizzarla e quindi meglio diffondere i propri prodotti rispetto alle imprese concorrenti. La necessità di mettere in circolazione messaggi pubblicitari veritieri e trasparenti rappresenta un obbligo che i professionisti hanno nei confronti del consumatore[6] quale motore che alimenta il mercato e la produzione di massa[7]. La figura ed il ruolo del consumatore, tuttavia, tendono a variare nel corso del tempo[8], così come variano i suoi bisogni[9], influenzati da vari fattori[10].

---

nell'era digitale, Milano, 2022; A. SIROTTI GAUDENZI, *Proprietà intellettuale, diritto industriale e information technology*, Milano, 2022; ID., *Manuale pratico dei marchi e dei brevetti*, Sant'Arcangelo di Romagna, 2019; L. TREVISAN e G. CUONZO, *Proprietà industriale, intellettuale e IT*, Milano, 2022; AA.VV., *Proprietà intellettuale*, a cura di F.A. GENOVESE e G. OLIVIERI, Torino, 2021; L.C. UBERTAZZI, *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, Padova-Milano, 2019; AA.VV., *Concorrenza, mercato e diritto dei consumatori*, a cura di G. CASSANO, A. CATRICALÀ e R. CLARIZIA, Torino, 2018.

[3] Durante il Rinascimento, tra il XV e il XVI secolo, si sviluppano i traffici commerciali internazionali che recano seco la necessità di declamare i pregi di un prodotto, incarico svolto dai venditori ambulanti e dagli imbonitori nei mercati e nelle fiere. Da un punto di vista commerciale, con le prime «società di capitali», nasce la figura del mercante-imprenditore che opera in mercati internazionali con la movimentazione di merci in volumi superiori rispetto all'artigiano. Sul mercato iniziano a farsi strada i beni di lusso (come oro e pietre preziose) e prodotti esotici (ad es. il cacao o i tulipani), importati da luoghi lontani grazie ai progressi della navigazione; di contro si assiste ad un progressivo divario tra luogo di produzione e di consumo si allontanano. Al crescere della produzione aumenta dunque la necessità di vendere in luoghi distanti e, pertanto, di identificare e distinguere il prodotto per provenienza e caratteristiche attraverso la «marca».

[4] La seconda metà dell'Ottocento costituisce la base storica, economica e culturale per la nascita della pubblicità moderna. Da un lato lo sviluppo industriale ed il progresso tecnologico, consentono l'ingresso nel mercato di un'ingente quantità di prodotti, dall'altro si assiste ad un progressivo aumento dell'urbanizzazione e delle prime vendite di massa e con condizioni standardizzate (a prezzo fisso e visibile). Sulla stampa, appannaggio di chi era in grado di leggere, iniziano a comparire delle inserzioni, piccoli annunci di vendita ad es. di prodotti curativi; in un primo momento si tratta d'inserzioni gratuite che dopo diventeranno a pagamento.

[5] Si trattava, perlopiù, di una pubblicità che faceva leva sulla grafica e sulle immagini e caratterizzata da semplicità ed immediatezza. Anche dal punto di vista del contenuto, il messaggio pubblicitario veniva declinato usando spesso la forma imperativa dei verbi: «chiedete», «prendete», «bevete», ecc.

[6] Da un punto di vista tassonomico-legale, il consumatore o utente è «la persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta», mentre il professionista è, specularmente, «la persona fisica o giuridica che agisce nell'esercizio della propria attività imprenditoriale, commerciale, artigianale o professionale, ovvero un suo intermediario» (art. 2, lett. a) e c), D.Lgs. 6 settembre 2005, n. 206).

[7] Cfr. AA.VV., *Marketing: mercati, prodotti e relazioni*, a cura di R. GRANDINETTI, Roma, 2016.

[8] Ai giorni nostri, «il consumatore, (…), è certamente diverso da quello che seguiva le prime pubblicità televisive, nel senso che questi è maggiormente informato sulle caratteristiche del prodotto e su quelli succedanei ma in grado di soddisfare le proprie personali esigenze. Ne consegue che in una società sempre più informata, in cui le notizie viaggiano sulla fibra ottica e non più soltanto attraverso il passaparola (…), si è quindi passati ad una funzione diversa, da informazione a persuasione, oramai prevalente (*moral suasion*), specie con i monopoli e le multinazionali». Così V. VITOLO, *Il sistema dei rapporti d'impresa ed i nuovi soggetti del mercato*, in R. VITOLO e M. IMBRENDA, *Profili sistemici dei rapporti giuridici d'impresa*, Milano, 2020, 14.

A tal proposito non si è mancato di osservare come i «cambiamenti sociali, la nascita delle nuove tecnologie, la creatività hanno portato alla nascita di un nuovo consumatore che non si pone più in maniera acritica e passiva nei confronti di chi comunica»[11]. In suo favore, secondo alcuni, si manipola il concetto di consumo, «tanto che il consumatore diviene partner e committente (…) in un rapporto che – grazie alla tecnologia – può anche essere di collaborazione e co-creazione»[12]. Questo consum-attore[13] pone attenzione all'intera filiera della produzione di beni che acquista, sino al suo

[9] Da un punto di vista economico, il bisogno è uno stato d'insoddisfazione, causato dalla divergenza tra la condizione attuale di un individuo ed il suo stato desiderabile, innescato da stimoli interni o esterni. Detto concetto va tenuto necessariamente distinto da quello di desiderio, specifico ed influenzabile da diverse variabili, che consiste nell'individuazione di qualcosa di specifico in grado di soddisfare i bisogni. Tale *quid* è un prodotto ben definito che, quindi, funge da mezzo particolare. I bisogni, a differenza dei desideri, sono generici e non influenzabili; questi vengono suddivisi in due macro-aree: i bisogni innati – o detto altrimenti primari – e i bisogni appresi o acquisiti, detti anche secondari. I primari si caratterizzano in relazione alla loro necessaria soddisfazione per la sopravvivenza dell'individuo come, ad es., nutrirsi o dormire. I secondari, invece, sono il risultato dell'interazione dell'individuo con l'ambiente.

[10] Secondo il *Rapporto Coop* 2012, in *italiani.coop*, le famiglie italiane hanno modificato le loro abitudini di consumo, alla luce dell'aumento delle persone sole o delle coppie senza figli, dell'aumento dell'aspettativa di vita e dell'età media, dell'abbassamento del tasso di natalità nonché della crisi economica del 2008 che ha generato il calo del reddito reale delle famiglie italiane, l'aumento del tasso di disoccupazione e un generale clima di sfiducia nei confronti del futuro. Nove anni dopo, a seguito dei noti eventi pandemici, il quadro che emerge dal rapporto 2021, *ivi*, si presenta diverso: è principalmente l'ambiente ad attirare l'attenzione dell'opinione pubblica e, quindi, il mercato odierno – nell'ottica di una visione rivolta alle tematiche ambientali – richiede una sempre maggiore disposizione di materie alternative che vanno di pari passo con materie prime sempre più costose e meno disponibili. Nel rapporto 2024, *ivi*, il potere d'acquisto nel nostro Paese ritorna ai livelli pre-pandemia e si registra la diminuzione degli italiani che hanno vissuto situazioni di disagio importanti; questo come contropartita di un aumento di ore lavorate (un miliardo e mezzo), scende, di 4 punti percentuali, la quota di chi guarda con fiducia al futuro, che scende di 4 punti in due anni mentre aumenta il timore del futuro (di 11 punti percentuali), anche in relazione a possibili scenari di guerra. In questo scenario, prosegue il rapporto 2024, ci si approccia ai consumi in un'ottica di risparmio: l'essenziale diventa centrale ed il superfluo viene drasticamente ridotto; a caratterizzare la percezione di se stessi, inoltre, è la dimensione personale e privata per l'85% del campione piuttosto che la capacità economica e/o lo *status* sociale.

[11] B. GARGIULO, *Il nuovo consumatore*, in *La comunicazione ambientale: sistemi, scenari e prospettive. Buone pratiche per una comunicazione efficace*, a cura di E. BALZARETTI e ID., Milano, 2009, 157 ss.

[12] B. PAGAMICI, *Impresa ibrida e terzo settore. I modelli imprenditoriali innovativi per l'impresa di domani*, Padova, 2017, 62.

[13] Il termine è stato utilizzato fin dai primi anni 2000, v. ad es. S. GNASSO e G.P. PARENTI, *L'approccio generazionale come evoluzione del "marketing dell'esperienza"*, in *Le età della Tv. Indagine su quattro generazioni di spettatori italiani*, a cura di P. AROLDI e F. COLOMBO, Milano, 2004, 23; M.R. ZORINO, *Il consum*Attore, Padova, 2006. Il lemma si è poi diffuso, anche per indicare la consapevolezza del consumatore riguardo a tematiche come il commercio equo e solidale, fino a definirlo «guardiano del mercato» (l'espressione è di D. ARCIDIACONO, *Da suddito a guardiano del mercato: il ruolo del consumatore per la Csr*, in AA.VV., *La Responsabilità Sociale oltre l'impresa*, a cura di C. AREZZO, R. D'AMICO e S. RANDONE, Milano, 2008, 218 ss.). M. IMBRENDA, *Nuove tecnologie e dinamiche regolatorie dell'autonomia privata*, in AA.VV., *Frontiere digitali del diritto*, a cura di ID., S. PIETROPAOLI, G. DALIA e R.M. AGOSTINO, Torino, 2021, 116, rileva come l'applicazione della tecnologia blockchain «consente di monitorare il processo produttivo e quindi orientare le proprie scelte di consumo sulla base delle informazioni e dei riscontri acquisiti. In altre parole, l'uso attivo e critico degli algoritmi offre al consumatore delle "potenzialità emancipative", ponendolo in condizione – proprio attraverso una struttura decentrata, quale la *blockchain*, come tale democratica esplicazione, a sua volta, della sussidiarietà orizzontale – di contribuire come "consum-attore" all'efficienza del mercato»; ID., *Persona e scelte di consumo fra conoscenze neuroscientifiche e nuove frontiere tecnologiche*, in *Actual. jur. iberoam.*, 2021, 14, 831; C. LOSAVIO, *Il consumatore di alimenti nell'Unione europea e il suo diritto ad essere informato*, Milano, 2007, 235. L.P. VECCHIO, *Il consumatore diventa "consum-attore"(?)*, relazione al convegno *Cliente sostenibile, logistica sostenibile: cambia il paradigma tra costo e valore*, Politecnico di Torino, 5.11.2018, ritiene ancora debole una relazione tra sensibilità alle tematiche del trasporto delle merci e pratiche di consumo più sostenibili, sottolineando di contro l'inerzia dell'abitudine (al riguardo v. anche D. RUTIGLIANO, *E-commerce vincente. Dai modelli di business alle strategie di vendita online*, Milano, 2017).

smaltimento[14], finendo per tradursi in un interesse alle materie prime, alla tutela dei lavoratori e delle istanze ambientali, o per dirla altrimenti alla responsabilità sociale dell'impresa[15].

A fronte di questo «ottimismo» sul consumatore, non si è mancato di osservare – pragmaticamente – che il consumatore non è così autonomo e potente rispetto al sistema produttivo, potendo sì partecipare a numerosi processi di rielaborazione dei prodotti e dei messaggi ad essi relativi, grazie alle nuove tecnologie comunicative, ma la sua partecipazione è limitata per lo più a scelte effettuate all'interno di possibilità rigidamente definite; i consumatori, pertanto, pur essendo maggiormente coinvolti nei processi produttivi, continuano a rimanere all'interno del loro ruolo[16].

L'avvento della società dei consumi non riguarda, naturalmente, i soli consumatori maggiorenni, ma involve anche i minori che rivesto un ruolo sicuramente maggiore nel mercato e che, come conseguenza non certo positiva, si accompagna al c.d. fenomeno di patrimonializzazione dell'infanzia[17] («commodification of childhood»). È un dato di comune esperienza, infatti, che i minori rappresentino un segmento rilevante in vari settori merceologici, con conseguente ripercussione su spesa e capacità economica delle famiglie e dei minori stessi. Ciò ha comportato la nascita e l'incremento di specifiche strategie di marketing[18], dovute anche alla nuova

---

[14] Cfr. B. PAGAMICI, *op. loc. ult. cit.*

[15] *Ibidem*. Questa categoria di consumatori «è identificabile come quel gruppo che mostra un'attenzione per le questioni che riguardano gli espetti etici del consumo e che avverte l'esigenza sempre più generalizzata di effettuare un acquisto che sia ragionato, non bulimico, ma dettato da valori molto più forti e meno superficiali» (B. PAGAMICI, *op. cit.*, 64).

[16] Cfr. V. CODELUPPI, *Il mito del consum-attore*, in *Cultura e comunicazione*, 2011, 2, 12 ss.

[17] Cfr. A. VIVARELLI, *I minori nel rapporto di consumo e la «patrimonializzazione» dell'infanzia*, in *Corti salernitane*, 2022, 45 ss. *A contrario*, sulla depatrimonializzazione del diritto civile, v. C. DONISI, *Verso la «depatrimonializzazione» del diritto privato*, in *Rass. dir. civ.*, 1980, 644 ss.; A. DE CUPIS, *Sulla «depatrimonializzazione» del diritto privato*, in *Riv. dir. civ.*, 1982, II, 482 ss.; P. PERLINGIERI, *«Depatrimonializzazione» e diritto civile*, ora in ID., *Scuole tendenze e metodi. Problemi del diritto civile*, Napoli, 1989, 175 ss. Il passaggio da una concezione patrimonialistica ad una personalistica, al lume della Costituzione, prima, e del diritto euro-unitario, poi, «conduce al superamento di un diritto civile panpatrimoniale, avente a fondamento la proprietà privata, l'impresa, le ragioni del mercato, a favore di un diritto civile ispirato al valore primario della dignità della persona, dell'eguaglianza e della solidarietà» (così P. PERLINGIERI, *Interpretazione ed evoluzione dell'ordinamento*, in *Riv. dir. priv.*, 2011, 164). Si giunge a tale risultato anche «grazie al parallelo ruolo svolto dalle Corti costituzionali europee (compresa quella italiana) a difesa dei diritti dell'uomo, si passa dalla tutela del mercato quale tutela di consumatori e produttori ad un sistema di protezione dei diritti fondamentali della persona in quanto tale» (ID., *Le ragioni del mercato e le ragioni del diritto. Dalla Comunità economica europea all'Unione europea*, Lecce, 28.11.2007, in *service.unibas.it*, 32).

[18] Il *medium* riveste particolare rilevanza: è stato infatti osservato che i bambini sono più propensi a comprendere l'intento commerciale di una pubblicità televisiva, piuttosto che di un annuncio all'interno di giochi online (sulla legittimità di un provvedimento che vieta lo sfruttamento commerciale di giochi simulanti atti di violenza, in quanto contrari alla dignità della persona, v. C. Giust. UE, 14.10.2004, C-36/02, Omega Spielhallen- und Automatenaufstellungs-GmbH c. Oberbürgermeisterin der Bundesstadt Bonn, in *www.curia.europa.eu* e in *Giust. civ.*, 2005, I, 1435 ss.). La Commissione europea ha da ultimo avviato un'azione coordinata nei confronti di un'azienda del settore dei videogiochi per pratiche commerciali potenzialmente scorrette, cfr. *La Commissione e le autorità nazionali adottano misure per proteggere i minori da pratiche dannose nei videogiochi*, a cura della Rappresentanza in Italia, in *www.italy.representation.ec.europa.eu*, 21.03.2025. In Svizzera dall'1.01.2025, invece, gli operatori che metteranno a disposizione film o videogiochi dovranno stabilire e indicare in modo ben visibile l'età minima richiesta per ogni contenuto nonché procedere ad un controllo dell'età (a mente della l. federale del 30 settembre 2022).
Secondo l'art. 31 c. cons., la televendita non deve esortare i minorenni a stipulare contratti di compravendita o di locazione di prodotti e di servizi né arrecare pregiudizio morale o fisico ai minorenni. La

percezione del ruolo del minore. Nell'attuale società, interattiva e interconnessa, i minori rilasciano dati proprio come gli adulti (magari proprio dai dispositivi elettronici di questi ultimi), dati attraverso i quali è possibile generare introiti, guidando i gusti e le scelte, generando meccanismi di induzione all'acquisto[19] dovuti anche alla difficoltà a riconoscere la pubblicità online[20] e a reagire alle lusinghe commerciali[21].

---

disposizione risponde al principio generale secondo cui il minore non dovrebbe essere destinatario di comunicazioni commerciali scorrette o aggressive, in quanto lo stesso si trova in uno stato di asimmetria informativa (*rectius* formativa) rispetto all'operatore commerciale. Misure specifiche sono poi dettate dal Codice di autoregolamentazione TV e minori (in *www.mimit.gov.it*), come ad es. elementi di discontinuità ben riconoscibili e distinguibili dalla normale programmazione. V. anche gli artt. 20 e 21 c. cons. che qualificano rispettivamente come scorrette quelle pratiche commerciali idonee a falsare in misura apprezzabile il comportamento economico di un gruppo di consumatori particolarmente vulnerabili alla pratica o al prodotto cui essa si riferisce a causa della loro età o ingenuità ed ingannevoli quelle che possano minacciare la sicurezza di minori ed adolescenti, anche solo indirettamente. Dal canto suo il Codice di autodisciplina della comunicazione commerciale, in *www.iap.it*, nella sua versione vigente (dal 30.10.2024), all'art. 11, oltre a dettare regole specifiche, impone particolare cura nei messaggi diretti ai bambini, *i.e.* infra-dodicenni, e agli adolescenti, facendo divieto di abusare della «loro naturale credulità o mancanza di esperienza, o del loro senso di lealtà» o danneggiando il loro benessere psico-fisico.

[19] A tacere di ulteriori e più gravi pericoli che possono integrare condotte penalmente rilevanti.

[20] Un discorso a parte, poi, deve farsi per le cc.dd. piattaforme social e, più in generale, relativamente all'accesso all'offerta diretta di servizi della società dell'informazione: l'art. 8 del Reg. UE n. 2016/679 ha previsto il consenso del minore che abbia compiuto i sedici anni al trattamento dei suoi dati personali, mentre il D.Lgs. 10 agosto 2018, n. 101, ha abbassato la soglia a quattordici anni. A mente del Considerando 38 del GDPR, i dati personali del minore sono meritevoli di «specifica protezione (…), in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali». La giurisprudenza amministrativa ha affermato che la registrazione alla piattaforma ha natura contrattuale e la cessione dei dati personali da parte dell'utente costituisce la controprestazione (cfr. T.A.R. Lazio, 10.01.2020 e C. St., 29.03.2021, n. 2631, entrambe in *www.giustizia-amministrativa.it*; v. E. TOSI, *Dati personali e contratto: un ossimoro apparente*, in *EJPLT*, 2023, 2, 71 ss., consultabile al sito: https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1911/1458; P. TANDA, *I nuovi orizzonti della nozione di* privacy *e la patrimonializzazione dei dati personali da parte dei* social network, in *Dir. proc. amm.*, 2020, 731 ss.). Secondo un'interessante prospettiva, poi, nei casi di IA c.d. generativa non potrebbe parlarsi di atti di vita quotidiana o di scarsa rilevanza, per cui si ammette generalmente la capacità di agire del minore, quanto piuttosto «di un contratto di rilevante importanza, il cui oggetto, per sua natura, comporta rischi rilevanti per i rapporti di educazione ed istruzione dei minori con i genitori, i tutori e gli insegnanti» (S. ORLANDO, *I lividi dei minorenni* sparring partners *di ChatGPT e l'età minima per attivare il servizio in Italia*, in *Pers. mer.*, 2023, 1, 4); il minore sarebbe esposto al rischio di «lacune e deficit di formazione di una capacità critica indispensabile per la crescita, lo sviluppo e l'impiego di facoltà intellettuali necessarie per operazioni come la redazione di riassunti e di composizioni creative in modo autonomo» (*ivi*). Del resto l'armonico formarsi della personalità del minore non potrebbe certamente dirsi sprovvisto di riferimenti al vertice del nostro sistema ordinamentale (cfr. gli artt. 2 e 31, co. 2, Cost., laddove la Repubblica si assume il compito di proteggere «l'infanzia e la gioventù» nello svolgimento della loro personalità). Tanto porta poi ad interrogarsi sul contenuto degli obblighi d'istruzione ed educazione dei figli in capo agli esercenti la responsabilità genitoriale, a mente degli artt. 30 Cost., 147 e 2047 c.c. (cfr. anche il d.l. 30.04.2020, n. 28).
In favore di un nuovo concetto di vulnerabilità, avulso da deficit fisio-psichici della persona umana, legato proprio alla condizione di esseri umani che si muovono in un ambiente digitale appare indispensabile in una prospettiva di sviluppo equilibrato delle tecnologie in tutte le direzioni possibili secondo L. GATT e I.A. CAGGIANO, *Consumers and digital environments as a structural vulnerability relationship*, in *EJPLT*, 2022, 2, 8 ss., consultabile al sito: https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1724/1239.

[21] In dottrina, v. *amplius* C. MURGO, *L'identità personale dei minori, tra responsabilità genitoriale e capacità di autodeterminarsi*, in *EJPLT*, 2024, 2, 115 ss., consultabile al sito: https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1994/1628; R. SENIGAGLIA, *Rischi identitari per la persona minore d'età nell'ambiente digitale*, in *EJPLT*, 2023, 2, 62 ss., consultabile al sito: https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1909/1457; G. ZICCARDI, *I minori online tra videogiochi e metaverso*, in AA.VV., *I minori nella società digitale tra rischi e nuove opportunità*, a cura di S. STANCO, in *Ciberspazio e dir.*, 2023, 3, 325 ss.; A. ROSSETTI, *La vita dei bambini negli ambienti digitali*, Torino, 2023; G. PERFETTI, *L'educazione del minore al consumo digitale, consapevole e sostenibile: quale ruolo per i genitori?*, in *Actual. jur. iberoam.*, 2022, 17 *bis*, 1398 ss.; G. CAPILLI, E-commerce *e minori*, *I contratti del*

2. Caratteri della pubblicità commerciale nel prisma della rilevanza costituzionale del mercato.

Il legislatore, nel riconoscere la libertà di concorrenza tra imprese quale corollario del diritto alla libera iniziativa economica privata (art. 41 Cost.)[22], non può venir meno alla tutela del mercato e dei soggetti che vi operano, non solo gli altri imprenditori ma anche i consumatori che si rivolgono al mercato e che hanno il diritto a compiere scelte libere e consapevoli (v. artt. 2, 41, co. 2, Cost.)[23]; pertanto, la concorrenza diventa una ricerca di massimizzazione del benessere dei consumatori, nonché, tramite la tutela della struttura concorrenziale del mercato, del raggiungimento del benessere sociale inteso come efficienza allocativa, produttiva ed innovativa[24].

La dottrina non manca di sottolineare come la Costituzione repubblicana avesse già riconosciuto la rilevanza del mercato, pur non facendone espressa menzione nella sua formulazione originaria. Dunque, «di mercato, di concorrenza (…) non [si] fa esplicita menzione e [la Costituzione] sul punto, pertanto, è tacciata, ma ingiustamente, di ambiguità. In essa la difesa del mercato sussiste ed è di alto profilo; si collega più che alle ragioni dell'economia a quelle della politica in funzione di garanzia della democraticità dell'insieme», ossia del sistema, «e quindi come avversione alla collettivizzazione dei beni di produzione e alla pianificazione centralizzata e autoritaria»[25]. L'art. 41 Cost., come autorevole dottrina rammenta[26], non si limita a sancire la mera libertà di iniziativa economica privata (co. 1), ma precisa al contempo, con estrema chiarezza, la necessità di un controllo e che tale iniziativa privata viene subordinata alla realizzazione dell'utilità sociale e che soprattutto non può esercitarsi in contrasto con l'ambiente, la salute, la libertà, la dignità e la sicurezza umana (co. 2); pertanto le leggi del mercato incontrano necessariamente dei valori che non sono mercantili e il costituente

---

consumatore, a cura di ID., Torino, 2021, 167 ss.; P. STANZIONE, *Capacità e minore età nella problematica della persona umana*, Napoli, 2018 (rist. 1975); I.A. CAGGIANO, *L'età del consenso e il trattamento dei dati personali dei minori*, in C. FABBRICATORE, A. GEMMA, G. GUIZZI, N. RASCIO e A. SCOTTI (a cura di), *Liber amicorum per Paolo Pollice*, Torino, 2020, 83 ss.

[22] L'inquadramento costituzionale della pubblicità si basa sul rapporto tra manifestazione del pensiero e l'esercizio di un'attività economica; le due libertà non sono però poste sullo stesso piano, in quanto quella di libera manifestazione del pensiero gode di una protezione più intensa in termini di applicazione concreta (v. E. APA, *La pubblicità commerciale*, Napoli, 2011, 95). La pubblicità commerciale costituisce attività d'impresa anche per la giurisprudenza (cfr. C. Cost., 17.10.1985, n. 231, in *www.cortecostituzionale.it* e Cass., 23.11.1999, n. 12993, in *Giust. civ.*, 2000, I, 31 ss. con nota di RAMPONE, *La pubblicità commerciale tra libertà di manifestazione del pensiero e libertà di iniziativa economica*). Cfr. anche S. GATTI, *Pubblicità commerciale*, cit., 1058.

[23] In questi termini S. GATTI, *op. cit.*, 1059. In proposito, *ex plurimis*, v. anche il pensiero di P. PERLINGIERI, *Interpretazione ed evoluzione dell'ordinamento*, cit., 64; A. GATTO, *Consumatore e "persona"*, in *Dir. vivente*, 2016, 2, 54 ss.; S. ROSSI, *Il mercato e i diritti sociali*, *I diritti sociali dal riconoscimento alla garanzia: il ruolo della giurisprudenza*, a cura di E. CAVASINO, G. SCALA e G. VERDE, in *Quaderni del Gruppo di Pisa*, 2013, 8 ss., in *www.gruppodipisa.it*; V. BUONOCORE, *Iniziativa economica privata e impresa*, in *Iniziativa economica e impresa nella giurisprudenza costituzionale*, a cura di ID., in *Cinquant'anni della Corte Costituzionale nella Repubblica italiana*, XVI, Napoli, 2006, 47 ss.

[24] Cfr. V. NATALINI, *Il principio della libera concorrenza*, in *Profili sistemici*, cit., 477.

[25] P. PERLINGIERI, *Mercato, solidarietà e diritti umani*, ora in ID., *Il diritto dei contratti fra persone e mercato. Problemi di diritto civile*, Napoli, 2003, 239 ss.

[26] *Ex plurimis* v. V. BUONOCORE, *Iniziativa economica*, cit., 3 ss. e ID., *Etica degli affari e impresa etica*, in *Giur. comm.*, 2004, I, 181 ss., ove ha osservato che all'art. 41 Cost. viene delineato «un modello d'impresa apportatore di benessere per la comunità e rispettoso dei più elementari diritti della persona umana».

ha inteso attribuire priorità alla persona e ai suoi diritti fondamentali rispetto all'impresa, alla produzione e al mercato[27].

La concorrenza, poi, assume una nuova luce con la riforma del Titolo V della II Parte della Costituzione[28] che finisce con esplicitare la rilevanza costituzionale del mercato[29]. La versione attuale dell'art. 117 Cost., infatti, non si limita a ripartire le competenze legislative tra Stato e Regioni, ma prevede un obbligo positivo di promozione del mercato e della concorrenza[30]. La giurisprudenza costituzionale ha avuto modo di precisare come lo Stato abbia poteri di intervento diretto sul mercato ricorrendo ad un'accezione di concorrenza, intesa in senso «dinamico» e «trasversale» quale concetto che identifica interventi promozionali «misure pubbliche volte a ridurre squilibri, a favorire le condizioni per un sufficiente sviluppo del mercato o ad instaurare assetti concorrenziali»[31].

Viene da sé, pertanto, la rilevanza anche – e ai fini di quanto ci occupa soprattutto – giuridica della pubblicità da considerare come «pratica commerciale» con dei requisiti ben precisi, vale a dire riconoscibilità (palese), verità e correttezza (v. art. 2 D.Lgs. n. 145/2007). Palese: tale requisito attiene alla capacità della stessa di essere chiaramente riconoscibile, vietando di conseguenza ogni tipo di messaggio pubblicitario subliminale o occulto. Veritiera: il messaggio pubblicitario deve essere trasmesso secondo il principio di ragionevolezza[32], fornendo le informazioni e dati sufficienti ed esatti del prodotto in questione, che deve risultare ben determinato e definito nelle sue caratteristiche. Corretta: svolta nel rispetto delle norme, del buon costume e senza arrecare danno ai consumatori e alle imprese concorrenti.

Il messaggio pubblicitario, in primo luogo, deve essere riconoscibile come tale e distinguibile, ad esempio da articoli di giornale o riviste periodiche. Secondo la giurisprudenza di merito[33], infatti, non è consentito sfruttare la

---

[27] Cfr. P. PERLINGIERI, *Le ragioni del mercato*, cit., 34.

[28] L. cost. 3 ottobre 2001, n. 3.

[29] Cfr. P. PERLINGIERI, *op. loc. ult. cit.* Secondo l'a. «se mantenessimo l'architettura della Repubblica ed eliminassimo l'iniziativa economica privata, avremmo una Repubblica diversa, fondata o sulla collettivizzazione dei beni di produzione o sul liberismo economico sfrenato» (*ivi*, 35).

[30] In tal senso, ad es., B. LIBONATI, *Ordine giuridico e legge economica del mercato*, in AA.VV., *Scritti in onore di Antonio Pavone La Rosa*, I, 2, Milano, 1999, 657. In senso contrario v. N. IRTI, *L'ordine giuridico del mercato*, Roma-Bari, 2003, 28 ss. Si registra, infine, la posizione intermedia di chi ritiene che il combinato disposto degli artt. 3 e 41 Cost. non tutelerebbe in via diretta la concorrenza, essendo questa ricavabile «per il tramite della tutela dell'individuo nei confronti delle formazioni monopolistiche» (A. BALDASSARRE, *Iniziativa economica privata*, in *Enc. dir.*, XI, Milano,1971, 602, nota 59).

[31] Così C. Cost., 18.12.2004, n. 14, in *www.cortecostituzionale.it* e, *ex plurimis*, in *Regioni*, 2004, 978 ss. con nota di CARANTA, *La tutela della concorrenza, le competenze legislative e la difficile applicazione del Titolo V della Costituzione*; in *www.associazionedeicostituzionalisti.it*, 2004, con nota di SACCO, *Competenze statali trasversali e potestà legislativa regionale: un tentativo di razionalizzazione (a proposito della "tutela della concorrenza") della Corte costituzionale.* Cfr. anche M. FIERRO, *La tutela della concorrenza nei giudizi di legittimità costituzionale in via principale (2002-2015)*, Studio 280, in *www.cortecostituzionale.it*, 2015.

[32] Avverte la dottrina che il concetto di ragionevolezza è storico e relativo, né si risolve unicamente «nella tecnica, pur ampiamente utilizzata, dell'interpretazione funzionale e della valutazione comparativa degli interessi, ma richiede l'interpretazione assiologicamente orientata di ogni disposizione o fatto giuridicamente rilevante, sí da perseguire una soluzione conforme al sistema giuridico di riferimento e ai suoi principi» (così G. PERLINGIERI, *Ragionevolezza e bilanciamento nell'interpretazione recente della Corte Costituzionale*, in *Actual. jur. iberoam.*, 2019, 10, 36).

[33] Trib. Palermo, sez. imprese, 3.05.2018, in *Dir. ind.*, 2019, 347 ss., con nota di GHINI, *Copertine «pubblicitarie» di quotidiani e sfruttamento della capacità diffusiva del quotidiano.*

«capacità diffusiva» del giornale con cover plastificate, che altro non sono che spazi pubblicitari, che inglobano il quotidiano: lo sfruttamento è stato ravvisato «nella vendita di spazi pubblicitari su supporti cartacei inseriti nella copertina in p.v.c. trasparente e nella successiva distribuzione della stessa presso gli esercizi commerciali»[34]. L'Autorità garante per la concorrenza e il mercato (AGCM)[35], dal canto suo, è intervenuta tempo addietro per sanzionare una nota rivista automobilistica e una società produttrice per pubblicità occulta, giacché gli articoli (con veste grafica e articolazione tipica di un «pezzo» giornalistico)[36], «sono diretti esclusivamente ad elogiare le caratteristiche dei veicoli (…) in modo del tutto acritico (…), ed addirittura recano un esplicito invito all'acquisto della gamma (…)»[37].

Allo stato, la pubblicità ingannevole è disciplinata dal codice del consumo (artt. 18 ss.) per tutelare i consumatori da pratiche commerciali scorrette e/o aggressive, dal D.Lgs. 2 agosto 2007, n. 145, che tutela i professionisti nei casi di pubblicità ingannevole e comparativa scorretta e dal codice di autodisciplina pubblicitaria (le cui norme sono vincolanti solo nei confronti di chi le abbia accettate, *ex* art. 27 *ter* c. cons.).

Già il codice civile, *in nuce*, contiene norme per contrastare la concorrenza sleale tramite pubblicità ingannevole – che prima del 1992 – non era espressamente regolata; si ricorreva a quanto previsto dal numero tre dell'art. 2598 c.c. che reputa concorrenza sleale la condotta di chi «si vale direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda»[38].

---

[34] Trib. Palermo, sent. n. 2105/2018, cit. Secondo il collegio, «la copertina trasparente di per sé considerata non sarebbe di alcun interesse per gli operatori commerciali, i quali mai acquisterebbero gli spazi pubblicitari, se non fosse per l'evidente legame tra la stessa e il quotidiano di volta in volta considerato. La copertina, quindi, diventa mero strumento mediante il quale la (…) sfrutta la capacità diffusiva del quotidiano per pubblicizzare quelle imprese a cui essa ha concesso uno spazio pubblicitario a titolo oneroso» (*ivi*).

[35] L'Autorità è stata istituita con l. 10.10.1990, n. 287, con una serie di poteri in materia di concorrenza e di abuso di posizione dominante in ambito nazionale e si raccorda con i corrispondenti organi UE. Al fine di tutelare la concorrenza e il mercato, l'Autorità può esercitare poteri d'indagine ed ispettivi, adottare provvedimenti ed irrogare le sanzioni previste dalla legge. Chiunque vi abbia interesse può segnalare all'Autorità eventuali violazioni, tra l'altro, del D.Lgs. n. 206/2005 (cfr. art. 37 *bis* c. cons.). Se a seguito dell'attività istruttoria, l'Autorità ravvisa delle infrazioni, fissa alle imprese ed agli enti interessati il termine per l'eliminazione delle stesse ed eventualmente applica una sanzione amministrativa pecuniaria; i provvedimenti dell'AGCM sono ricorribili, a mente dell'art. 135 c.p.a., al T.A.R. del Lazio. Nel caso in cui la questione riguardi materie di competenza di altre Autorità (ad es. comunicazioni, assicurazioni, ecc.), l'AGCM nella propria istruttoria acquisisce (anche) i relativi pareri.

[36] E inoltre privi del riquadro con l'indicazione «informazione pubblicitaria».

[37] AGCM, provv. 9.11.2011, n. 22953, in *Boll.* n. 45/11, in *www.agcm.it*. Gli articoli in questione, secondo l'Autorità Garante nel provvedimento citato, andavano inquadrati «nell'ambito di un'iniziativa posta in essere con una stretta interazione tra le Parti, avente ad oggetto l'intera campagna pubblicitaria, che ha incluso anche inserzioni a pagamento (…) e comportato un sensibile incremento del fatturato pubblicitario di (…) nei confronti della casa automobilistica [che] è stata in grado di verificare e concordare previamente il contenuto degli articoli di cui trattasi».

[38] La norma viene pensata in origine per regolamentare in via generale la comunicazione aziendale, *i.e.* in tutte le forme che essa può assumere. Si consideri, tuttavia, che all'entrata in vigore del codice civile, i mezzi di comunicazione disponibili erano ben diversi da quelli attuali. La giurisprudenza riconosce pacificamente la natura di norma aperta della fattispecie *de quo*, spettando al giudice riempirla di contenuti «avuto riguardo alla naturale atipicità del mercato ed alla rottura della regola della correttezza commerciale» (Cass., 6.06.2022, n. 18034, in *Sole24Ore - Sist. doc.*). Mette, inoltre, conto osservare che anche di fronte a violazioni di norme pubblicistiche non si è *ex se* in presenza di un atto sleale di concorrenza, «dovendosi distinguere tra norme volte a porre limiti all'esercizio dell'attività imprenditoriale, la cui violazione è sempre riconducibile entro il paradigma contemplato da detta disposizione, e norme che

Tuttavia, la dottrina riteneva che il rimedio non fosse sufficientemente ampio per contrastare la pubblicità ingannevole[39] e soltanto con il D.L.gs. 25 gennaio 1992, n. 74[40], il legislatore introduceva tale divieto allo «scopo di tutelare dalla pubblicità ingannevole e dalle sue conseguenze sleali i soggetti che esercitano un'attività commerciale, industriale, artigianale o professionale, i consumatori e, in genere, gli interessi del pubblico nella fruizione di messaggi pubblicitari» (art. 1).

Per pubblicità si intende: «qualsiasi forma di messaggio che sia diffuso, in qualsiasi modo, nell'esercizio di un'attività commerciale, industriale, artigianale o professionale allo scopo di promuovere la vendita di beni mobili o immobili, la costituzione o il trasferimento di diritti ed obblighi su di essi oppure la prestazione di opere o di servizi». È, invece, ingannevole «qualsiasi pubblicità che in qualunque modo, compresa la sua presentazione, induca in errore o possa indurre in errore le persone fisiche o giuridiche alle quali è rivolta o che essa raggiunge e che, a causa del suo carattere ingannevole, possa pregiudicare il loro comportamento economico ovvero che, per questo motivo, leda o possa ledere un concorrente» (art. 2). La disciplina della pubblicità è poi confluita nel codice del consumo; in particolare l'art. 19 c. cons., nella sua prima formulazione, riprendeva l'art. 1 del D.Lgs. n. 74/1992 con l'aggiunta del riferimento alla pubblicità comparativa: l'obiettivo del codice è di tutelare non soltanto il consumatore finale ma tutti i soggetti impegnati nei vari livelli della filiera produttiva; tale disciplina, pertanto, non coincide solamente con il diritto dei consumatori, essendo applicabile sia ai contratti di consumo sia d'impresa[41].

---

impongono costi alle imprese operanti sul mercato, la cui violazione non costituisce di per sé l'illecito in parola, occorrendo che l'imprenditore che si duole degli atti del concorrente ne dimostri l'attitudine potenzialmente lesiva dei propri diritti, mediante malizioso ed artificioso squilibrio delle condizioni di mercato» (Cass., ord. 8.05.2023, n. 12049, in *One LEGALE*). L'art. 2598 c.c. contempla la tutela risarcitoria anche in riferimento ad atti preparatori di concorrenza sleale, a patto che venga dimostrata l'esistenza di un danno eziologicamente collegato a questi ultimi; nel caso in cui «il pregiudizio riguardi l'immagine e l'apprezzamento che i consumatori nutrono per i prodotti commercializzati con un determinato segno distintivo, il risarcimento è parametrato, oltre che sul danno emergente e sul danno non patrimoniale, anche sul danno da lucro cessante, sempreché la condotta lesiva abbia determinato una contrazione dei ricavi del danneggiato o abbia avuto, comunque, un'incidenza sul relativo importo» (Cass., ord. 8.03.2023, n. 6876, in *One LEGALE*).

[39] Cfr. G. Floridia, *La tipizzazione normativa*, in P. Auteri, Id., V. Mangini, G. Olivieri, M. Ricolfi e P. Spada, *Diritto Industriale. Proprietà intellettuale e concorrenza*, Torino, 2012, 357. V. anche la critica di P. Perlingieri, *Le ragioni del mercato*, cit., 34 che ritiene «limitata e impropria» la disciplina codicistica della concorrenza. S. Gatti, *Pubblicità commerciale*, cit., 1059, avvertiva l'assenza di una «norma da cui poter derivare una tutela generale e completa». V. anche la pur autorevole, sebbene risalente, opinione di chi riteneva possibile l'interesse dei consumatori realizzabile indirettamente nel quadro della repressione della concorrenza sleale (cfr. T. Ascarelli, *Teoria della concorrenza e dei beni immateriali*, Milano, 1960, 185 e 217).

[40] Provvedimento normativo emanato in attuazione della dir. n. 84/450/CEE, come modificata dalla dir. n. 97/55/CE.

[41] Tuttavia la versione attuale del codice del consumo riguarda le «pratiche commerciali scorrette tra professionisti e consumatori poste in essere prima, durante e dopo un'operazione commerciale relativa a un prodotto, nonché alle pratiche commerciali scorrette tra professionisti e microimprese». Invece, per le microimprese la tutela in detta materia è assicurata in via esclusiva dal D.Lgs. n. 145/2007. Sui contratti del consumatore, *ex plurimis*, v. Aa.Vv., *Manuale di diritto dei consumi*, a cura di G. Perlingieri, L. Mezzasoma e M. Angelone, Napoli, 2024; A. Barenghi, *Diritto dei consumatori*, Padova-Milano, 2024; G. De Cristofaro, *Diritto italiano ed europeo dei consumatori. Studi*, Padova-Milano, 2024; B. Parenzo, *La profilazione algoritmica nel prisma dell'autonomia privata*, Napoli, 2024; A. Senatore, *I contratti del consumatore*, in Aa.Vv., *Lineamenti di Diritto Privato nell'era dell'economia digitale*, a cura di M. Imbrenda, Padova-Milano, 2023.

Elementi necessari alla definizione di un'attività scorretta sono l'idoneità della pubblicità a indurre in errore i suoi destinatari e a pregiudicare il comportamento economico del consumatore che riceve il messaggio. Le fattispecie di illecito previste dalla norma hanno un carattere puramente oggettivo, atteso che prescindono completamente dalle categorie della colpa o del dolo[42], e rendono dunque irrilevante l'intenzionalità del professionista a diffondere informazioni che possano qualificare una pubblicità come ingannevole; è richiesta, infine, l'effettiva possibilità che un acquirente possa cadere in errore (*i.e.* la sua potenzialità). Il codice del consumo, nella sua versione attuale, considera ingannevole (art. 21) «una pratica commerciale che contiene informazioni non rispondenti al vero o, seppure di fatto corretta, in qualsiasi modo, anche nella sua presentazione complessiva, induce o è idonea ad indurre in errore il consumatore medio (…) e, in ogni caso, lo induce o è idonea a indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso»[43].

Gli elementi considerati dalla norma sono:

a) l'esistenza o la natura del prodotto;

b) le caratteristiche principali del prodotto[44];

c) la portata degli impegni del professionista, i motivi della pratica commerciale e la natura del processo di vendita, qualsiasi dichiarazione o simbolo relativi alla sponsorizzazione o all'approvazione dirette o indirette del professionista o del prodotto;

d) il prezzo o il modo in cui questo è calcolato o l'esistenza di uno specifico vantaggio quanto al prezzo;

e) la necessità di una manutenzione, ricambio, sostituzione o riparazione;

f) la natura, le qualifiche e i diritti del professionista o del suo agente[45];

g) i diritti del consumatore, incluso il diritto di sostituzione o di rimborso.

Il legislatore, al co. 2, considera ingannevole una pratica commerciale che, nella fattispecie concreta, e tenuto conto di tutte le caratteristiche e circostanze del caso, induce o è idonea ad indurre il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso e comporti una qualsivoglia attività di commercializzazione del prodotto che ingenera confusione. Stessa considerazione riceve il mancato rispetto da parte del professionista degli impegni contenuti nei codici di condotta che il medesimo si è impegnato a rispettare, ovvero ancora una qualsivoglia attività di marketing che promuova un bene, in uno Stato membro dell'Unione europea, come identico a un bene commercializzato in altri Stati

---

[42] V. S. SICA e V. D'ANTONIO, *Pubblicità ingannevole e comparativa*, in Aa.Vv., *Commentario del Codice del consumo. Inquadramento sistematico e prassi applicativa*, a cura di P. STANZIONE e G. SCIANCALEPORE, Milano, 2006, 104.

[43] Si noti come il codice del consumo ponga attenzione alla fattispecie concreta di potenziale «scorrettezza» della comunicazione pubblicitaria, senza rifarsi solo a dati puramente formali. In tema cfr. la giurisprudenza del Consiglio di Stato, *ex plurimis* v. C. St., 2.12.2024, n. 9614; 14.05.2024, n. 4297 e 19.03.2024, n. 2665, tutte in *www.giustizia-amministrativa.it*.

[44] Quali la sua disponibilità, i vantaggi, i rischi, l'esecuzione, la composizione, gli accessori, l'assistenza *post*-vendita al consumatore e il trattamento dei reclami, il metodo e la data di fabbricazione o della prestazione, la consegna, l'idoneità allo scopo, gli usi, la quantità, la descrizione, l'origine geografica o commerciale o i risultati che si possono attendere dal suo uso, o i risultati e le caratteristiche fondamentali di prove e controlli effettuati sul prodotto.

[45] Quali l'identità, il patrimonio, le capacità, lo *status*, il riconoscimento, l'affiliazione o i collegamenti e i diritti di proprietà industriale, commerciale o intellettuale o i premi e i riconoscimenti.

membri, mentre questo bene ha una composizione o caratteristiche significativamente diverse, salvo fattori legittimi e oggettivi.

Dunque, riassuntivamente, per pratiche commerciali s'intendono tutti i comportamenti dei professionisti oggettivamente correlati alla promozione, vendita o fornitura di beni o servizi, posti in essere anteriormente, contestualmente o anche posteriormente all'instaurazione dei rapporti contrattuali[46]. La condotta materiale tenuta dal professionista può consistere in dichiarazioni, atti materiali, o anche semplici omissioni (nei casi in cui le regole di diligenza impongano una condotta commissiva). Le «pratiche commerciali scorrette» costituiscono un *genus* unitario di illecito[47], all'interno del quale il legislatore ha regolato due diversi sottotipi (e all'interno, due ulteriori fattispecie presuntive) che si pongono in rapporto di specialità[48] rispetto alla prima: le pratiche ingannevoli e le pratiche aggressive.

La portata della norma viene estesa a «qualsiasi bene, servizio, diritto e obbligazione» (art. 18 che reca la definizione di prodotto) e la lett. d) dell'art. 18 c. cons. include tutte le forme di promozione, commercializzazione dei prodotti sia vecchie sia nuove, perciò sia i messaggi pubblicitari veri e propri che altre attività di comunicazione di impresa[49]. Un secondo profilo della condotta ingannevole è dato dalle omissioni ingannevoli (art. 22 c. cons.) che i professionisti possono tenere riguardo ad informazioni rilevanti, inducendo così il consumatore a prendere decisioni distorte; l'omissione può riguardare sia informazioni occulte, presentate in modo ambiguo o incomprensibile, intempestive o non indicanti l'intento commerciale. Il terzo co. dell'art. 22 prevede che nel caso in cui il mezzo di comunicazione impiegato imponga «restrizioni in termini di spazio o di tempo» occorrerà tener conto come di ogni altra misura che i professionisti possono adottare per informare i consumatori con altri mezzi.

All'attività pubblicitaria si applicano i canoni di «buona fede, correttezza e lealtà» sanciti dall'art. 39 c. cons., quale espressione di un unico principio di correttezza.

Affinché il mercato e la concorrenza funzionino correttamente è necessario che i consumatori ricevano informazioni che permettano loro di scegliere in modo consapevole tra i differenti prodotti e servizi disponibili sul mercato. La pubblicità ingannevole è, invece, idonea a danneggiare la concorrenza, giacché sposta l'attenzione dei consumatori sui prodotti promossi in modo illecito. L'interpretazione del pregiudizio sul cliente è da ricercarsi unicamente nell'idoneità della pubblicità di influenzare il comportamento del consumatore e non in un danno patrimoniale od economico. Inoltre, si ricorre

---

[46] Il legislatore del 2023, D.Lgs. 7 marzo 2023, n. 26, ha poi qualificato come scorretta la pratica commerciale di banche, istituti di credito ed intermediari finanziari che obbligavano il consumatore a sottoscrivere una polizza assicurativa ovvero ad aprire un conto corrente presso il professionista ai fini dell'erogazione di un mutuo.

[47] AA.VV., *Pratiche commerciali scorrette e codice del consumo. Il recepimento della direttiva 2005/29 Ce nel diritto italiano (decreti legislativi nn. 145 e 146 del 2 agosto 2007)*, a cura di G. DE CRISTOFARO, Torino, 2008, 97 ss.

[48] Per specificazione.

[49] La prima tipologia di messaggi pubblicitari, che usano gli strumenti classici come televisione, radio, stampa, cinema ed internet, viene anche indicata come comunicazione above the line. Gli altri mezzi di comunicazione aziendale sono definiti below the line e riguardano principalmente sponsorizzazioni, pubbliche relazioni, passaparola, social media.

al principio del «primo contatto»[50], ovvero al principio secondo il quale l'ingannevolezza deve essere valutata con riferimento al primo contatto con i consumatori senza tener conto di eventi successivi, che possono rendere nulli gli effetti del messaggio per i consumatori. Già nel 2003[51] l'Autorità garante ha ritenuto ingannevole un messaggio pubblicitario su un sito internet, all'interno del quale veniva proposto un servizio gratuito per il download di brani musicali senza esplicita indicazione degli oneri previsti. L'Autorità ha specificato che l'operatore è obbligato ad esporre nel messaggio, in modo chiaro ed evidente, fin dal primo contatto gli oneri e le condizioni generali di contratto del servizio pubblicizzato[52].

Come si è detto in precedenza, la tutela dalle pratiche commerciali scorrette, pur essendo rivolta a tutti gli operatori del mercato, è principalmente indirizzata al cosiddetto consumatore medio. Il legislatore comunitario ha inteso fare proprio questo concetto, proveniente della letteratura economica, per riferirsi a quel soggetto «normalmente informato e ragionevolmente attento ed avveduto, tenendo conto di fattori sociali, culturali e linguistici»[53]. La Commissione ha precisato, nella relazione illustrativa della proposta di direttiva n. 2005/29/CE, che il criterio adottato costituisce espressione del principio di proporzionalità e deve essere applicato quando una pratica commerciale è destinata alla maggior parte dei consumatori. La direttiva non è rivolta soltanto al consumatore medio ma tutela anche quei consumatori particolarmente vulnerabili alle pratiche commerciali scorrette. Nel Considerando 19, infatti, si chiarisce che quando alcune caratteristiche, tra cui l'età, l'infermità o ingenuità del gruppo di consumatori in oggetto li rendano particolarmente vulnerabili al comportamento scorretto, la tutela deve essere indirizzata al membro medio del gruppo. Ne deriva che nel valutare la slealtà di una pratica occorre tenere conto dell'influenza sul consumatore medio comune o sul consumatore medio del gruppo[54].

---

[50] P. AUTERI, *La disciplina della pubblicità*, in ID., G. FLORIDIA, V. MANGINI, G. OLIVIERI, M. RICOLFI e P. SPADA, *Diritto industriale*, cit., 401.

[51] V. AGCM, provv. 24.07.2003, n. 12276, in *Boll.* n. 30/03, in *www.agcm.it*.

[52] Secondo l'Autorità garante nel provv. n. 12276/03, cit., «il messaggio, dunque, così come risulta strutturato, lascia intendere che la connessione con il sito dell'operatore avvenga sulla rete Internet, al costo della chiamata effettuata per la navigazione in rete. Ne (*sic*) viene riportata alcuna informazione circa il fatto che, una volta aderito al contratto, avviene l'immediata disconnessione alla rete del proprio fornitore di accesso ad Internet e l'automatico instradamento del traffico al numero telefonico a valore aggiunto "709", i cui costi sono esplicitati soltanto all'interno dell'ultima finestra con barra di scorrimento laterale, con caratteri di piccole dimensioni. Al riguardo, si rileva che la dicitura "*L'utente ha il dovere di leggere condizioni e costi contenuti all'interno del software di connessione*", riportata nella pagina iniziale, a caratteri di dimensione ridotta e senza alcun richiamo nel corpo principale della pagina Internet segnalata, contrariamente a quanto sostenuto dall'operatore, non chiarisce, sin dal primo momento in cui si instaura il contatto con il consumatore, che l'utilizzo del programma di scaricamento di brani musicali comporta un unico percorso che coinvolge due soggetti distinti, a costi onerosi (…). Tali sottaciute circostanze, (…) rendono il messaggio gravemente carente di informazioni di rilievo, decisive per orientare le scelte di adesione o meno al servizio reclamizzato» (*ivi*).

[53] V. Considerando 18, dir. n. 2005/29/CE.

[54] Da ultimo cfr. C. Giust. UE, 14.11.2024, C-646/22, Compass c. AGCM, in *www.curia.europa.eu*; in *Riv. dir. eco. trasp. amb.*, 2024, 995 ss., con nota di G. MATTARELLA, *Polizze abbinate a finanziamenti, consumatore medio e pratiche commerciali scorrette*, in *www.giureta.unipa.it*. Secondo la Corte, «la nozione di "consumatore medio", ai sensi [della dir. n. 2005/29/CE], deve essere definita con riferimento a un consumatore normalmente informato nonché ragionevolmente attento ed avveduto. Una siffatta definizione non esclude tuttavia che la capacità decisionale di un individuo possa essere falsata da

3. Il sistema rimediale.

È risaputo che il nostro sistema ordinamentale è caratterizzato dalla presenza di una duplicità di livelli di tutela avverso la pubblicità sleale: pubblicistica e civilistica. Quello di matrice pubblicistica tutela gli interessi collettivi ed economici dei consumatori ed è preordinato a garantire l'efficienza e il buon funzionamento del mercato interno (cfr. art. 41 Cost.). La l. 10.10.1990, n. 287, ha istituito un organo pubblico indipendente, l'Autorità Garante della Concorrenza e del Mercato, dotata di una serie di poteri in materia di concorrenza e di abuso di posizione dominante in ambito nazionale e si raccorda con i corrispondenti organi UE. Al fine di tutelare la concorrenza e il mercato, l'Autorità può esercitare poteri di indagine ed ispettivi, adottare provvedimenti ed irrogare le sanzioni previste dalla legge. Chiunque vi abbia interesse può segnalare all'Autorità eventuali violazioni (cfr. art. 37 *bis* c. cons.).

Sotto l'aspetto civilistico, l'ermeneutica prevalente ritiene che la scorrettezza della pratica commerciale non sia *ex se* ragione sufficiente a creare una nuova ipotesi di invalidità del contratto ovvero causa di recesso *ad nutum* da parte del consumatore[55]. L'attenzione della dommatica si è soffermata sulla questione degli effetti che la violazione del divieto di ricorrere a pratiche commerciali scorrette determina sulla validità del contratto concluso con il consumatore. I rimedi, sinteticamente, sono stati individuati nella nullità del contratto «a valle» ovvero nell'applicazione della c.d. nullità di protezione[56]; nella possibilità di annullamento e, infine, nella c.d. teoria dei vizi incompleti[57].

Mette conto segnalare, inoltre, l'intervento del legislatore comunitario che già dal 2015[58] ha iniziato a pensare (o a ripensare) diversi strumenti di tutela per modernizzare in chiave digitale il diritto dei consumatori. Il culmine si è avuto nel 2019, anno con le dir. nn. 770 e 771, relative rispettivamente ai contratti per la fornitura di contenuti e servizi digitali e ai contratti di vendita di beni, e la dir. n. 2161[59], denominata *omnibus* per il suo scopo di voler

---

limitazioni, quali distorsioni cognitive». Nella prospettiva del giudice amministrativo cfr. C. St., 17.05.2024, n. 4402, e 17.05.2024, n. 4422, entrambe in *www.giustizia-amministrativa.it*.

[55] Non potendosi ritenere superato il principio generale dell'art. 1372 c.c., secondo il quale il contratto non si scioglie che per mutuo consenso o per le cause ammesse dalla legge.

[56] V. ad es. C. SARTORIS, *Nullità di protezione e interesse ad agire*, Padova-Milano, 2022; S. POLIDORI, *Nullità di protezione e sistematica delle invalidità negoziali*, Napoli, 2016; G. PERLINGIERI, *La convalida delle nullità di protezione e la sanatoria dei negozi giuridici*, Napoli, 2011.

[57] Per le varie soluzioni offerte dalla dommatica v., *ex multis*, a AA.VV., *Codice del consumo commentato*, a cura di V. CUFFARO, Milano, 2019; T. FEBBRAJO, *Il* private enforcement *del divieto di pratiche commerciali scorrette*, Napoli, 2018; V. RICCIUTO, *Le pratiche commerciali scorrette nella contrattazione a distanza*, in *Riv. dir. impr.*, 2015, 1 ss.; A. FACHECHI, *La pubblicità, le pratiche commerciali e le altre comunicazioni* in AA.VV., *Diritti e tutele dei consumatori*, a cura di G. RECINTO, L. MEZZASOMA e S. CHERTI, Napoli, 2014, 45 ss.; M. LIBERTINI, *Clausola generale e disposizioni particolari nella disciplina delle pratiche commerciali scorrette*, in *Contratto e impresa*, 2009, 73 ss.; AA.VV., *Le pratiche commerciali sleali. Direttiva comunitaria ed ordinamento italiano*, a cura di E. MINERVINI e L. ROSSI CARLEO, Milano, 2007.

[58] Cfr. COMMISSIONE EUROPEA, *Strategia per il mercato unico digitale in Europa*, 6.05.2015, COM(2015) 192, e *Un "*New Deal*" per i consumatori*, 11.04.2018, COM(2018) 183.

[59] Sulla dir. n. 2019/2161 v., *ex plurimis*, E. BATTELLI, *Questioni aperte in materia di contrattazione nelle piattaforme online*, in *Contratti*, 2022, 5, 563 ss.; G. VERSACI, *Le tutele a favore del consumatore digitale nella "direttiva* omnibus*"*, in *Pers. merc.*, 2021, n. 3, 583 ss.; I. SPEZIALE, *La Dir. 2019/2161/UE tra protezione dei consumatori e promozione della competitività sul mercato unico*, in *Corr. giur.*, 2020, 4, 441 ss.

modernizzazione delle norme dell'Unione in materia di protezione dei consumatori. Come i primi commentatori hanno rilevato, «[a]l *public enforcement* già sperimentato, il legislatore europeo ha voluto quindi associare l'introduzione di un più efficace apparato di diritti e rimedi esercitabili sul piano orizzontale»[60].

La direttiva prevede poi un ulteriore elemento di novità in tema di conseguenze privatistiche della violazione del divieto di pratiche commerciali sleali: a mente del nuovo art. 11 *bis*, aggiunto alla dir. UE n. 2005/29, «i consumatori lesi (...) devono avere accesso a rimedi proporzionati ed effettivi, compresi il risarcimento del danno e, se pertinente, la riduzione del prezzo o la risoluzione del contratto»[61]. Il legislatore nazionale, nel recepire la dir. UE n. 2161/2019[62], ha sostanzialmente ripreso l'espressione utilizzata dal legislatore comunitario e ai sensi del comma 15 *bis* dell'art. 27 c. cons. è possibile adire il giudice ordinario[63], tuttavia, il legislatore non ha indicato una gerarchia la scelta del rimedio da attivare spetta quindi al singolo consumatore[64].

La tutela individuale si affianca, inoltre, allo strumento collettivo dell'azione di classe come modificata dalla l. 12.04.2019, n. 31 che se ha spettro più ampio rispetto al regime precedente continua ad essere uno strumento utilizzabile per la tutela del consumatore.

A ricevere tutela, tuttavia, è anche il professionista/imprenditore leso dalle tecniche pubblicitarie *latu sensu* scorrette: in tale ipotesi l'intervento dell'AGCM potrebbe non essere efficace come deterrente[65] ed i rimedi pubblicistici non essere sufficienti a ripristinare la situazione giuridica compromessa dalla pratica commerciale scorretta. Il rimedio pubblicistico, pertanto, può essere integrato da quello privato, essendo pacifico che la pratica sleale integra gli estremi di un illecito civile[66], azionabile dinanzi al giudice ordinario. Pertanto, il rimedio risarcitorio[67] si affianca agli altri

---

[60] Così VERSACI, *op. cit.*, 584.

[61] SPEZIALE, *op. cit.*, ritiene che l'intervento costituisca un passo in avanti rispetto all'art. 3, dir. UE n. 2005/29, che si limita a consentire, o meglio a non pregiudicare «l'applicazione del diritto contrattuale, in particolare delle norme sulla formazione, validità o efficacia di un contratto». La stessa a., *ivi*, osserva che La scelta finale in merito alle specifiche possibilità da rendere disponibili nel singolo Paese UE, essendo rimessa ancora al legislatore nazionale, si traduce nel fallimento di quell'ambizioso tentativo di armonizzazione massima della direttiva del 2005.

[62] Con il d.lgs. 7.03.2023, n. 26.

[63] «I consumatori lesi da pratiche commerciali sleali possono altresì adire il giudice ordinario al fine di ottenere rimedi proporzionati ed effettivi, compresi il risarcimento del danno subito e, ove applicabile, la riduzione del prezzo o la risoluzione del contratto, tenuto conto, se del caso, della gravità e della natura della pratica commerciale sleale, del danno subito e di altre circostanze pertinenti. Sono fatti salvi ulteriori rimedi a disposizione dei consumatori.».

[64] il risarcimento del danno o lo scioglimento del vincolo negoziale sono la «condizione minima» richiesta dalla dir. UE n. 2161/2019 secondo SPEZIALE, *op. cit.*

[65] È la stessa Autorità Garante a sottolinearlo nel provv. 4.08.2016, n. 26137, in *Boll.* n. 28/16, in *www.agcm.it*.

[66] La pronuncia dell'Autorità Garante può giovare all'attore quale elemento di prova sulla fondatezza dell'azione. Cfr. Cass., 10.12.2013, n. 27527 e 14.08.2014, n. 17971, entrambe in *One LEGALE*.

[67] Il rimedio risarcitorio per gli atti di concorrenza sleale è del resto già previsto dall'art. 2600 c.c. La concorrenza sleale tramite pubblicità viene sanzionata anche dall'art. 2 del D.Lgs. n. 145/2007, quale atto atipico idoneo ad indurre in errore i consumatori e a pregiudicare il comportamento economico dei concorrenti. In tal senso, da ultimo, v. Trib. Ferrara, 7.02.2025, in *DeJure*, secondo cui la diffusione di pubblicità ingannevole, basata su affermazioni false o esagerate sulle qualità dei propri prodotti e rivolta indistintamente ai potenziali acquirenti, è in grado di alterare le dinamiche concorrenziali attraverso una comunicazione commerciale scorretta e potenzialmente dannosa per i consumatori e gli altri operatori del

strumenti di tutela offerti dall'ordinamento[68] per salvaguardare la concorrenza, anche in un'ottica – potenzialmente – deterrente e sanzionatoria[69].

La giurisprudenza amministrativa concorre a fissare i limiti della pubblicità ingannevole, ritenendo che vada considerata tale non solo la pratica commerciale attraverso la quale si trasmettono informazioni non corrispondenti al vero, ma anche quella che contiene un'informazione che, «seppure di fatto corretta, in qualsiasi modo, anche nella sua presentazione complessiva, induce o è idonea ad indurre in errore il consumatore medio» sugli elementi indicati dalla medesima disposizione, tra i quali, «il prezzo o il modo in cui questo è calcolato o l'esistenza di uno specifico vantaggio quanto al prezzo» (art. 21, lett. d), c. cons.)[70]. Nello stesso senso è stato statuito che «anche le modalità grafiche ed espressive con cui gli elementi del prodotto vengono rappresentati all'interno del messaggio rientrano tra gli standard di chiarezza, completezza e intelligibilità degli elementi rilevanti del prodotto, la cui mancanza può integrare una omissione ingannevole», giacché «la trasparenza della comunicazione commerciale contribuisce ad implementare l'efficienza del mercato attraverso la riduzione delle asimmetrie informative»[71]. Ne consegue che il carattere ingannevole di un messaggio pubblicitario può riguardare anche le modalità con cui si veicola un determinato bene o servizio, quando incidono sulla capacità di comprendere l'esatta natura di ciò che viene offerto, manipolando artificialmente il processo di selezione; a rilevare, quindi, è la valutazione del «primo impatto» che la comunicazione ha sul consumatore considerando tutti gli elementi (grafici e di contesto) che possono distogliere l'attenzione[72].

---

mercato ed integra un'ipotesi di concorrenza sleale atipica. È appena il caso di rammentare, tuttavia che si tratta pur sempre di un danno-conseguenza e dunque da provarsi secondo le regole ordinarie. V., in termini, Cass., ord. 18.02.2021, n. 4255, in *One LEGALE*, secondo cui «il danno cagionato dal compimento di atti di concorrenza sleale non è *in re ipsa* ma, essendo conseguenza diversa ed ulteriore rispetto alla distorsione delle regole della concorrenza, richiede di essere autonomamente provato secondo i principi generali che regolano il risarcimento da fatto illecito».

[68] Ad es. di natura cautelare, come l'ordine di interrompere una determinata campagna pubblicitaria, la pubblicazione della sentenza e via enumerando.

[69] Naturalmente in nome della correttezza delle affermazioni pubblicitarie non possono commettersi abusi. Ad es., quanto alla veridicità dell'informazione pubblicitaria, se fosse ipoteticamente possibile acquisire qualsiasi informazione allora il segreto aziendale, che pure riceve tutela ordinamentale, si troverebbe a rischio; si veda ad es. la scelta del legislatore del D.Lgs. 19 agosto 2005, n. 195, sul c.d. accesso ambientale che all'art. 5 esclude dette informazioni quando ciò rechi pregiudizio alla riservatezza delle informazioni commerciali o industriali, per la tutela di un legittimo interesse economico e pubblico, nonché ai diritti di proprietà industriale e intellettuale. Sui limiti al diritto d'accesso nelle procedure ad evidenza pubblica, v. T.A.R. Veneto, 5.11.2024, in *Foro amm.*, 2024, II, 1599 ss.

[70] Cfr. C. St., 8.02.2022, n. 879 e 14.09.2018, n. 5396, entrambe in *www.giustizia-amministrativa.it*.

[71] Cfr. C. St., 19.09.2017, n. 4378, in *www.giustizia-amministrativa.it*.

[72] In tal senso v. C. St., 25.03.2025, n. 2462, in *www.giustizia-amministrativa.it*.

4. Pubblicità (anche) come *medium* di manifestazione del pensiero.

La pubblicità non viene utilizzata soltanto per veicolare comunicazioni commerciali, offerte di prodotti, beni o servizi. Nel significato che ne dà il vocabolario, infatti, «pubblicità» significa anche «rendere pubblico, divulgare, diffondere tra il pubblico»[73]. Nelle scienze sociali, infatti, la pubblicità «può anche essere veicolo di comunicazioni di interesse sociale o mirare a ottenere l'adesione a un sistema ideologico (propaganda politica e religiosa)»[74].

Un'interessante e recente pronuncia del Consiglio di Stato[75] si occupa proprio di tale aspetto. La vicenda riguardava una campagna contraria all'utilizzo di una pillola abortiva, la c.d. pillola dei cinque giorni dopo, che ricorreva ad un'immagine shock creando un parallelismo tra l'utilizzatrice del medicinale e il noto personaggio di Biancaneve[76]. L'Onlus interessata, a fronte della delibera della giunta comunale che aveva negato l'affissione dei manifesti, ricorreva prima al T.A.R. e, successivamente, al Consiglio di Stato[77].

La disciplina comunale richiamava espressamente il codice di autodisciplina delle comunicazioni commerciali, le cui norme si applicano a «qualunque messaggio volto a sensibilizzare il pubblico su temi di interesse sociale» (art. 46, primo co.), prevedendo (al successivo terzo co.) che i messaggi, non devono, tra l'altro: «a) (…) ricorrere a richiami scioccanti tali da ingenerare ingiustificatamente allarmismi, sentimenti di paura o di grave turbamento; b) colpevolizzare o addossare responsabilità a coloro che non intendono aderire all'appello; c) presentare in modo esagerato il grado o la natura del problema sociale per il quale l'appello viene rivolto (…)». La sentenza di seconde cure depotenzia, inoltre, la critica al provvedimento amministrativo, presentato come censura, ritenendo come «la giurisprudenza della Corte europea dei diritti dell'uomo[78] (al pari della Corte costituzionale italiana) ha costantemente sottolineato che la libertà di espressione non sia illimitata e assolutamente non controllata, ma, comportando doveri e responsabilità, può essere sottoposta dall'autorità pubblica anche a formalità, condizioni ovvero restrizioni, le quali, proprio in una società democratica, appaiono misure necessarie a proteggere l'interesse pubblico superiore e la reputazione ovvero i diritti altrui»[79]. Si osserva ancora come la manifestazione del pensiero

---

[73] V. *Pubblicità*, in *Vocabolario online Treccani*, in *www.treccani.it*.
[74] V. *Pubblicità*, in *Enciclopedia online Treccani*, in *www.treccani.it*.
[75] C. St., 17.01.2025, n. 362, in *www.giustizia-amministrativa.it* e in *Dir. e giustizia*, 26.02.2025, con nota di CRISAFI, *Manifesti contro la pillola antiabortiva: legittimo lo stop del Comune*.
[76] Nella specie i manifesti ritraevano l'immagine di una donna stesa per terra, apparentemente priva di coscienza, con accanto una mela rossa.
[77] Dalla sentenza di secondo grado si ricava che sul manifesto, in caratteri più piccoli, era riportato, quasi come un *disclaimer*, il testo: «Campagna di sensibilizzazione promossa da (…) per la tutela del diritto fondamentale alla vita (art. 2 Cost.) e del diritto alla salute (art. 32 Cost.) sui rischi della somministrazione della pillola RU486. Questa affissione costituisce espressione del diritto alla manifestazione del pensiero (art. 21 Cost.) finalizzata a suscitare un dibattito plurale e la riflessione critica. Non è idonea a ledere diritti e libertà positivamente previsti dalla legge».
[78] Tuttavia la Corte EDU, 30.01.2018, ric. n. 69317/14, Sekmadienis c. Lituania, in *www.hudoc.echr.coe.int*, ha ritenuto che il principio della libertà di espressione si applichi anche a quelle che offendono, scioccano o disturbano (cfr. § 70 e la giurisprudenza ivi citata). Sul punto, tra i vari, v. N. COLAIANNI, *Quando la libertà prevale sulla morale: la pubblicità*, in *QG*, 1.03.2018 e M. CROCE, *Sekmadienis Ltd. c. Lithuania: luci ed ombre di una sentenza a favore della libertà di espressione nella pubblicità commerciale*, in *Quad. cost.*, 2018, 2, 325 ss.
[79] La sentenza richiama espressamente l'analogo precedente di C. St., 4.07.2024, n. 5930, in *www.giustizia-amministrativa.it*.

incontri non solo i limiti della violenza e dell'aggressività verbale, dovendosi attribuire pari rilevanza alla «continenza espressiva»[80] dei contenuti nonché dei principi di prudenza e precauzione volti ad evitare impatti sulla sensibilità dei fruitori del messaggio e a garantirne la chiara corrispondenza al vero; in tale duplice visione prospettica – di legalità e di rispetto della continenza espressiva – ben può l'amministrazione sindacare il contenuto e le modalità del messaggio[81].

Il richiamo fatto dalla PA ai d.lgs. n. 145 e n. 146 del 2 agosto 2007 appare al Consiglio di Stato perfettamente in termini, dato che si tratta di principi generali in materia di pubblicità, anche se riferiti ad attività commerciali. Detto altrimenti, secondo il supremo consesso amministrativo anche simili comunicazioni rivolte alla generalità dei consociati devono rispondere ai canoni di correttezza, trasparenza e verità. I limiti al contenuto delle affissioni, dunque, sono posti anche a tutela di interessi fondamentali della persona. Il potere di verifica e di controllo dell'amministrazione pubblica, pertanto, «è teso alla verifica di contenuti comunque suscettibili di arrecare pregiudizio ad altri soggetti, secondo un criterio di prudenza e precauzione»[82].

Per quanto, invece, riguarda la pubblicità di natura politica, anche in questo caso lo sviluppo dei mezzi d'informazione ha indotto il legislatore a regolare il loro utilizzo a scopo di propaganda nel periodo preelettorale, allo scopo di garantire il rispetto di condizioni di parità tra le liste e tra i candidati concorrenti, venendo in rilievo numerosi precetti costituzionali tra cui la libertà del voto (art. 48 Cost.) il diritto a partecipare democraticamente alla vita politica del Paese (art. 49 Cost.) e di manifestare le proprie opinioni politiche (art. 21 Cost.). È da premettere, in termini più generali, che il settore della «comunicazione politica» non ha dei confini netti. Infatti, pur riguardando aspetti di natura politica molte forme di comunicazione, anche attraverso mezzi digitali, non per questo possono essere considerate «politiche». Anche la qualifica dell'autore della comunicazione, inoltre, non è utile a schiarire il dubbio sulla riconducibilità alla «comunicazione politica», dal momento che che non ogni forma di questa scaturisce da esponenti del mondo politico o partitico[83].

Le fonti normative interne principali sono la l. 22 febbraio 2000, n. 28[84] e la l. 10 dicembre 1993, n. 515, che trova in parte applicazione anche nel caso di

[80] Che caratterizza la fisiologica dialettica democratica.

[81] Il giudice amministrativo non dubita, tuttavia, come il giudizio negativo sull'interruzione volontaria di gravidanza attenga «alla libertà di opinione e di libera manifestazione del pensiero»; tale giudizio, tuttavia, non può spingersi « fino al punto di sovrapporre ingannevolmente la contestata finalità del farmaco alla sua distribuzione e utilizzazione debitamente autorizzate».

[82] Così C. St. n. 5930 del 2024, cit.

[83] Cfr. E.A. ROSSI, *Problemi di coordinamento normativo nel contrasto alla disinformazione politica e commerciale*, in *federalismi.it*, 2025, 15, 78 ss.

[84] Sulla «attualità» della normativa citata cfr. G.E. VIGEVANI e M. CAZZANIGA, *Comunicazione politica e Costituzione tra televisione e piattaforme digitali*, in *medialaws.eu*, 2025, p. 14 ss. Nella giurisprudenza costituzionale v. C. cost. 7 maggio 2002, n. 155, in *www.cortecostituzionale.it* che ritiene la l. n. 28/2000 necessaria ad assicurare la conoscenza di informazioni da una pluralità di fonti ed a garantire una informazione il più possibile obiettiva e imparziale del cittadino. L'AGCOM, dal canto suo, osserva che «la televisione si conferma ancora il mezzo con la maggiore valenza informativa, sia per frequenza di accesso anche a scopo informativo, sia per importanza e attendibilità percepite» (*Rapporto sul consumo di informazione*, Roma, 2018, II).

elezione degli organi comunali[85]. Da un lato, la Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi detta, annualmente, gli indirizzi cui deve attenersi la RAI, quale concessionaria del servizio pubblico radiotelevisivo, dall'altro l'Autorità per le garanzie nelle comunicazioni[86] definisce le regole cui devono attenersi le emittenti radiofoniche e televisive nazionali e locali e gli organi di stampa periodica e quotidiana, vigilando della l. n. 28/2000 e comminando le relative sanzioni. In particolare, i messaggi politici elettorali a pagamento ricevono una specifica disciplina sia sulla carta stampata sia nelle radio e televisioni; i messaggi sui giornali devono essere riconoscibili, anche mediante specifica impaginazione ed in spazi chiaramente evidenziati, secondo modalità uniformi per ciascuna testata, e recare la dicitura «messaggio politico elettorale» indicando il soggetto committente.

A fronte della normativa nazionale, si segnala che il legislatore comunitario è intervenuto con il Reg. UE n. 2024/900[87] per contribuire al corretto funzionamento del mercato interno della pubblicità politica e servizi connessi nonché tutelare i diritti e le libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'UE, in particolare il diritto alla vita privata e la protezione dei dati personali (art. 1, par. 4); viene definita come «politica» la pubblicità che consista nella preparazione, collocazione, promozione, pubblicazione, consegna o diffusione, con qualsiasi mezzo, di un messaggio fornito normalmente dietro retribuzione o tramite attività interne o nell'ambito di una campagna di pubblicità politica «di, a favore o per conto di un attore politico[88]» oppure «possa e sia inteso a influenzare l'esito di un'elezione o referendum, un comportamento di voto o un processo legislativo o regolamentare, a livello dell'Unione, nazionale, regionale o locale» (art. 3, n. 2). Il regolamento non incide sul contenuto degli annunci pubblicitari politici né su altri aspetti della pubblicità politica, come ad es. la conduzione delle campagne politiche, che restano disciplinati da norme nazionali, né disciplina i contenuti sotto la responsabilità editoriale e le opinioni espresse a titolo personale. La pubblicità politica, inoltre, deve essere chiaramente individuata come tale[89] e includere informazioni su chi l'ha pagata, a quale consultazione sia collegata e se sono state utilizzate tecniche di targeting o di distribuzione degli annunci; ulteriori, come ad esempio informazioni sugli importi aggregati o sulla loro origine, sono fornite nell'avviso di trasparenza che deve essere incluso in ogni pubblicità politica o facilmente recuperabile da essa.

Se l'intervento del legislatore comunitario è stato favorevolmente salutato[90], non si è mancato tuttavia di esprimere qualche perplessità

---

[85] V. C. GIUNTA, *L'espressione del pensiero politico: comunicazione, propaganda, pubblicità*, in *federalismi.it*, 2025, 14, 21 ss. e ivi per ulteriore bibliografia.

[86] Supportata dai Comitati regionali per le comunicazioni.

[87] In *www.eur-lex.europa.eu*, e destinato ad essere applicato, ad eccezione degli artt. 3 e 5, dal 10 ottobre 2025. In dottrina, tra gli altri, cfr. C. GIUNTA, *L'espressione del pensiero politico: comunicazione, propaganda, pubblicità*, in *federalismi.it*, 2025, 14, 21 ss.; C. LOBASCIO, *Micro-targeting politico e protezione dei dati personali.Il Regolamento (UE) 2024/900*, in *Riv. it. inform. diritto*, 2025, 2, 205 ss., in *www.rivistaitalianadiinformaticaediritto.it*.

[88] Sia esso il singolo candidato o il partito.

[89] Ricorre, come per la pubblicità commerciale, la necessità che sia riconoscibile (o palese).

[90] Cfr. E. STELLA, *La disciplina in materia di pubblicità politica del regolamento (Ue) 2024/900*, in *Eurojus*, *www.rivista.eurojus.it*, 6.05.2024, 6 ss.

interpretativa[91], in particolare legata alle tematiche digitali[92]. In effetti su quest'ultimo aspetto le fonti europee sono invero numerose, dal GDPR al recente *AI Act*, recando inevitabilmente il rischio di interferenze tra le stesse. L'*AI Act* include tra i sistemi di intelligenza artificiale ad alto rischio anche quelli destinati ad incidere sulla comunicazione politica (cfr. All. III n. 8, lett. b), da ciò ne deriva l'applicabilità delle regole previste per questa tipologia di sistemi[93].

Inoltre, la comunicazione (anche politica) *online* è caratterizzata da una serie di peculiarità che complicano non di poco il panorama. Tra queste si registrano «il problema del pluralismo esterno *online*, considerati i pochi "colossi" che si spartiscono il mercato del digitale, la disinformazione, il tema molto attuale della c.d. privatizzazione della censura e del controllo preventivo sui contenuti postati dagli utenti (politici compresi)»[94]. Si pone, poi, il problema dei rimedi contro una pubblicità politica potenzialmente sleale[95] che nell'ambito civile potrebbero essere individuati, da un lato, nell'azione risarcitoria aquiliana[96] – al ricorrere naturalmente di tutti gli elementi costitutivi della fattispecie – e, dall'altro, dall'utilizzo di strumenti di tutela cautelari che possano interrompere la lesione[97].

Appare problematica l'estensione della disciplina consumeristica, alcuni hanno osservato che nella rete si assiste ad una radicale mutazione della rappresentanza politica e la chiave normativa risiederebbe nelle normative adottate dalle OTT, che avrebbero natura contrattuale nel solco degli artt. 1341 e 1342 c.c.; da ciò discenderebbe una sostanziale assimilazione fra le strategie di marketing adottate sul mercato dei beni e dei servizi e quelle utilizzate nella propaganda politica[98]. Un ruolo non secondario viene svolto dall'AGCOM che ha esercitato «un ruolo di impulso e di coordinamento tra i diversi attori operanti nel settore dell'informazione online per favorire

---

[91] Cfr. V. IAIA, *I complessi contorni della nozione di pubblicità politica alla prova delle elezioni europee 2024*, in *www.medialaws.eu*, 2024, in particolare riguardo alle c.d. «attività interne». Secondo l'a., «il Considerando 24 qualifica tautologicamente le attività interne come quelle attività svolte all'interno di un'entità che agisce per proprio conto e che possono influenzare l'esito di un'elezione o referendum, un comportamento di voto o un processo legislativo o regolamentare. Né vi sono ulteriori delucidazioni in merito a quale tipo di entità (se ad esempio occorra una forma societaria dotata di personalità giuridica o sia sufficiente una forma associativa) si rivolga il regolamento».

[92] *Ibidem* si fa l'esempio di un «messaggio di sostegno o di avversione verso un partito o attore politico sia pubblicato senza remunerazione da un influencer», restando comunque ferma «la necessità di garantire la libertà di espressione (anche politica), ai sensi degli artt. 21 Cost. e 11 della Carta dei diritti fondamentali dell'Unione europea» (*ivi*). V. anche Ed. CATERINA, *La disciplina delle campagne elettorali tra obsolescenza normativa e innovazioni tecnologiche*, in *Osservatorio sulle fonti*, 2025, 2, *osservatoriosullefonti.it*, 45 ss.

[93] Che ricomprendono il rispetto dei requisiti della sez. 2 del capo III assieme agli stringenti obblighi per i fornitori e per i *deployers*.

[94] In questi termini VIGEVANI e CAZZANIGA, *Comunicazione politica e Costituzione*, cit., 25.

[95] Tralasciando ipotesi in cui il messaggio integri condotte penalmente rilevanti (ad es. artt. 278, 595 e 596 *bis* c.p.).

[96] Oltre all'eventuale costituzione di parte civile in un procedimento penale – *ex lege* 8.02.1948, n. 47 sono civilmente responsabili anche il proprietario della pubblicazione e l'editore in solido con gli autori del reato – che può comportare, oltre al risarcimento *ex* art. 185 c.p., anche il versamento di una somma a titolo di riparazione che integra un'ipotesi di risarcimento sanzionatorio.

[97] Ad es. il ricorso agli artt. 669 *bis* ss. e (in via sussidiaria) 700 c.p.c.

[98] Cfr. A. CARDONE, *Profilazione a fini politico elettorali e tenuta della democrazia rappresentativa: una lezione per le riforme istituzionali e per la regolazione del pluralismo democratico in rete*, in A. ADINOLFI e A. SIMONCINI (cur.), *Protezione dei dati e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022, 157 e ss. e P. CIARLO, *Democrazia, partecipazione popolare e populismo al tempo della rete*, in *Rivista AIC*, 2018, II, 6-7.

l'autoregolamentazione su base volontaria ai fini di contrasto dei fenomeni di disinformazione online in generale e, nello specifico, della lesione della correttezza, dell'imparzialità e del pluralismo dell'informazione»[99]. Dal canto suo, l'AGCM ha proposto di estendere la disciplina della *par condicio* anche alle comunicazioni politiche online a delineare regole ivi contenute potrebbero essere imposte anche nella rete, proprio alla luce di una «crescente e avvertita esigenza di rendere effettiva la tutela del pluralismo anche sulle piattaforme digitali»[100]. E tuttavia queste ultime non sembrano avere un dovere di intervento per ripristinare «la parità delle armi» nella comunicazione politica, né sembra potersi configurare un dovere di intervento costituzionalmente imposto mentre appare forse più praticabile un ritorno alla originaria neutralità dei gestori delle piattaforme[101].

Alla luce di queste tematiche, e della crescente diffusione delle tecnologie digitali nei contesti elettorali, il legislatore si è mosso con una proposta di legge[102] per prevenire «l'alterazione o la manipolazione delle campagne elettorali e referendarie attraverso la diffusione di contenuti ingannevoli prodotti mediante sistemi di intelligenza artificiale» con il dichiarato scopo di preservare l'integrità del procedimento elettorale[103]. La proposta riprende le definizioni già viste in sede europea (cfr. art. 2) fissando allo stesso tempo il divieto di «creazione e la diffusione con ogni mezzo di contenuti ingannevoli o manipolati rivolti agli elettori, generati in tutto o in parte con sistemi di intelligenza artificiale (IA), riguardanti gli eletti, i candidati impegnati nelle competizioni elettorali, i partiti e i movimenti politici»[104]. Inoltre, è stato previsto da un lato un sistema di controllo in capo all'AGCOM[105] e la possibilità per la «vittima» delle alterazioni virtuali di ricorrere direttamente al gestore del sito o della piattaforma per chiederne la rimozione o l'oscuramento, nell'inerzia del gestore l'Autorità Garante, *inaudita altera parte*, può ordinare la rimozione o il blocco[106].

5. Osservazioni conclusive.

La mutata attenzione per le dinamiche del mercato, anche in chiave ambientale[107], sembra destinata a portare ad una revisione delle regole

---

[99] Così la delib. AGCOM 423/17/Cons., 3.
[100] AGCOM, *Impegni assunti dalle società esercenti le piattaforme on line per garantire la parità di accesso dei soggetti politici alle piattaforme digitali durante le campagne per il referendum popolare confermativo relativo al testo della legge costituzionale*, in *www.agcom.it*, 2020, 1.
[101] Cfr. G.E. VIGEVANI e M. CAZZANIGA, *Comunicazione politica e Costituzione*, cit., 27.
[102] Atto Camera n. 2212, in *camera.it*.
[103] La p.d.l. si colloca in un rapporto di complementarità con il Reg. UE n. 2024/900 che non affronta direttamente il tema della disinformazione *online* effettuata con i mezzi forniti dall'intelligenza artificiale.
[104] Anche se non ingannevoli, deve essere dichiarata la natura artificiale dell'eventuale messaggio politico (cfr. art. 2 della proposta).
[105] Che in caso di inottemperanza agli obblighi potrà applicare sanzioni amministrative nonché quelle accessorie del blocco dei siti utilizzati per attività illecite
[106] Art. 2 della p.d.l. che introduce l'art. 9 *sexies* alla l. n. 212/1956.
[107] Basti citare la politica europea del Green Deal e la normazione relativa, tra cui mette conto almeno menzionare le dir. UE n. 2022/1760, n. 2024/825 e n. 2024/1760. La materia ambientale non è negletta dalla civilistica, cfr., tra i vari, G. D'IPPOLITO, *Il diritto del greenwashing. Dalla pubblicità ingannevole alle nuove prospettive per consumatori e aziende*, Firenze, 2025, 181 ss.; V. ZAMPAGLIONE, *Climate change: towards global law?*, in EJPLT, 2025, 1, consultabile al sito

vigenti, avendo sempre come riferimento il ruolo della concorrenza «trasformandola in uno strumento di intervento attivo sui mercati»[108], pure sotto il profilo pubblicitario[109]. Un mercato efficiente non è funzionale solamente allo sviluppo economico ma amplia i diritti e le libertà fondamentali dei cittadini dando loro pratica attuazione[110]. La migliore sintesi, dunque, è da rintracciare nell'art. 41 della Costituzione che nel valorizzare la libera iniziativa economica privata[111] la assoggetta ai valori assiologici dell'ordinamento, vale a dire la persona umana da non ritenere avulsa dall'ambiente che lo circonda.

Il fenomeno pubblicitario, tuttavia, non va necessariamente limitato alla comunicazione commerciale, che pure ne occupa una parte considerevole, ma anche alla trasmissione di messaggi, pensieri, opinioni su vari aspetti della vita quotidiana, in una trama normativa non necessariamente limitata alla fonte legale o regolamentare ma anche a quella «convenzionale» dei codici di condotta[112], espressione della rilevanza dell'autonomia negoziale; quest'ultima, infatti, non riveste una funzione soltanto integrativa bensì un ruolo parimenti rilevante nella creazione di regole che disciplinano interessi di microsistemi sociali o economici. Nel settore della comunicazione pubblicitaria si avverte, dunque, la necessità di bilanciare il diritto alla manifestazione del pensiero, di professione religiosa (art. 19 Cost.) o di attività politica (cfr. art. 49 Cost.), che possono essere assoggettate a formalità, condizioni o restrizioni al fine di tutelare e garantire i diritti altrui[113], con gli altri diritti fondamentali. Il comune denominatore di tutte le comunicazioni, pertanto, sembra essere la correttezza del messaggio e la sua chiara identificazione come comunicazione rivolta al pubblico, indipendentemente dalla natura commerciale o meno del contenuto[114].

Lungi dall'essere l'indagine compiuta in ogni dettaglio, il settore della pubblicità – intesa in senso lato, per come detto nelle pagine che precedono – si presenta come uno scenario complesso dove si avverte sempre più la

---

https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/2100/1664; M.C. Reale, *Comunicare l'impegno per l'ambiente: le nuove regole europee contro il* greenwashing, in *Sociol. dir.*, 2024, 1, 105 ss.; V. Corriero, *I problemi civilistici del diritto dell'ambiente*, Napoli, 2024; M. Pennasilico, *La "sostenibilità ambientale" nella dimensione civil-costituzionale: verso un diritto dello "sviluppo umano ed ecologico"*, in *Riv. quad. dir. amb.*, 2020, 3, 4 ss. Sia permesso, infine, il rinvio ad A. Senatore, Green claims *e* greenwashing*: aree grigie nella pubblicità verde*, in *Riv. dir. bancario*, 2025, 2, II, 77 ss.

[108] Così AGCM, *Relazione annuale sull'attività svolta* nel 2024, in *www.agcm.it*, 2025, 6.

[109] Sulla declinazione ambientale della pubblicità v., *ex multis*, N. Berardi, Greenwashing *e comunicazione d'impresa*, in Aa.Vv., *ESG e sostenibilità d'impresa: novità normative, strumenti e modelli societari*, a cura di G. Taffari ed E. Giovine, Padova-Milano, 2024, 46; F. Bertelli, *Pratiche commerciali scorrette. Le asserzioni di sostenibilità e la Dir. 2024/825/UE*, in *Oss. dir. civ. comm.*, 2024, 2, 333 ss.; L. Zoboli, *Il* greenwashing *e la tutela della corretta comunicazione d'impresa*, in *Riv. dir. banc.*, 2024, I, 273 ss.; A.P. Seminara, *I limiti della comunicazione pubblicitaria nei rapporti* business to business*, tra vanti di ecosostenibilità e raffronti fuorvianti*, in *Danno e resp.*, 2023, 5, 657; B. Pozzo, *I* green claims*, l'economia circolare e il ruolo dei consumatori nella protezione dell'ambiente: le nuove iniziative della Commissione UE*, in *Riv. giur. ambiente*, 2020, 707 ss.

[110] Cfr. la *Relazione annuale* 2024 AGCM, cit., 8.

[111] Che comunque è in grado di apportare vantaggi e benessere a chi la persegue e a chi collabora (cfr. artt. 4 e 36 Cost.).

[112] Cfr. ad es. il codice di autodisciplina pubblicitaria o il codice di *Corporate Governance*.

[113] Cfr. C. St., n. 362/2025 e n. 5930/2024, cit.

[114] Si rammenta che l'adeguata informazione rientra tra i diritti fondamentali del consumatore, *ex* art. 2 c. cons., assieme a quello di pratiche commerciali svolte al lume dei principi di buona fede, correttezza e lealtà, questi ultimi principi – naturalmente – sembrano potersi applicare a tutti i tipi di comunicazione.

necessità della sensibilità di tutti gli operatori[115] e dell'interprete per enucleare, e tutelare, i diversi profili di libertà, civili ed economiche della persona[116], dando attuazione ai principi giuridici ordinamentali.

[115] Esperti pubblicitari inclusi.

[116] Cfr. C. Cost., 13.06.2024, n. 105, in *wwww.cortecostituzionale.it*, secondo cui «"[r]imuovere prontamente i fattori di pericolo per la salute, l'incolumità e la vita dei lavoratori costituisce (…) condizione minima e indispensabile perché l'attività produttiva si svolga in armonia con i principi costituzionali, sempre attenti anzitutto alle esigenze basilari della persona" (…). Esigenze basilari della persona (delle persone oggi esistenti, e di quelle che saranno) tra cui si annovera ora, esplicitamente, anche la tutela dell'ambiente». La solidarietà si contrappone (o si dovrebbe contrapporre) all'«indole "predatoria" dell'uomo in sé e dell'attività umana, in particolare nella sua declinazione economica e produttiva» (così F. CALISAI, *Attività di impresa, sostenibilità e comunicazione. Il* greenwashing*: forme di tutela e rimedi civilistici*, in *Rass. dir. civ.*, 2022, 487). V., inoltre, P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, Napoli, 2020, 526, secondo cui «ogni attività deve sia produrre occupazione, sia garantire un progresso sociale ed economico sostenibile, nel rispetto dei valori e delle identità culturali preesistenti, del paesaggio e dell'ambiente».

LIST OF AUTHORS OF THIS EJPLT ISSUE

ANAS ABU ALOUN – Associate Professor of Civil Law, Arab American University, Palestine.

GIOIA ARNONE – Postdoctoral Affiliated Researcher, Vrije Universiteit Brussel (VUB), Belgium.

GIOVANNI BATTAGLINO – Ph.D. candidate, University of Camerino, Italy. LAST-JD Ph.D. Candidate, Vrije Universiteit Brussel (VUB), Belgium.

ILARIA AMELIA CAGGIANO – Full professor of Private Law, Università degli Studi Suor Orsola Benincasa, Italy. Vice-director of the JM Centre of Excellence – ReCEPL4STAI, Università degli Studi Suor Orsola Benincasa, Italy.

CARLO CANDELORO CAMPANILE – Ph.D. student in National Ph.D. Course in Earth Observation, Universitò di Roma "La Sapienza", Italy.

ANNA CAPELLÀ I RICART – Postdoctoral Researcher, Universitat Autònoma de Barcelona, Spain.

GIOVANNA CAPILLI – Full Professor of Private Law, Università San Raffaele di Roma, Italy.

MARIA ANTONIA CIOCIA – Full Professor of Private Law, Università degli Studi della Campania Luigi Vanvitelli, Italy.

DAVIDE SILVIO D'ALOIA – Ph.D., Lawyer, Università degli Studi Suor Orsola Benincasa, Italy.

ANTONELLA DI CERBO – Officer, Autorità Garante per la Protezione dei Dati Personali, Italy.

VALENTINA DI GREGORIO – Associate Professor of Private Law, Università di Genova, Italy.

MARCOS DANIEL DI LORETO – Associate Professor of Private Law, Universidad Abierta Interamericana, Argentina.

LUCILLA GATT – Full Professor of Private Law and New Technologies Law, Università degli Studi Suor Orsola Benincasa, Italy. Director of the JM Centre of Excellence – ReCEPL4STAI, Università degli Studi Suor Orsola Benincasa, Italy.

ELENI GAVRIIL – Lecturer in International Economic Law and Human Rights, Neapolis University Pafos, Greece.

LUIGI IZZO – Ph.D. in Humanities and Technologies: an integrated researche path, Università degli Studi Suor Orsola Benincasa, Italy.

MARIA TERESA LO CONTE – Junior Researcher, Research Centre in European Private Law (ReCEPL), Università degli Studi Suor Orsola Benincasa, Italy. Ph.D. student, Università degli Studi di Roma "Tor Vergata", Italy.

ARTURO MANIACI – Associate Professor of Private Law, Università degli Studi di Milano, Italy.

MARIA EUGENIA MAZZARELLA – Ph.D. student, Scuola Superiore Meridionale, Italy.

LURDES VARREGOSO MESQUITA – Associate Professor, Polytechnic Universidade do Porto and Universidade Portucalense, Portugal. Researcher, Instituto Jurídico Portucalense, Portugal.

GEORGIOS PAVLIDIS – Associate Professor of International and EU Law UNESCO Chair, Neapolis University Pafos, Greece.

ENZA PELLECCHIA – Full Professor of Private Law, Università di Pisa, Italy.

STEFANIA PIA PERRINO – Postdoctoral Research Fellow in Private Law, Università di Milano Bicocca, Italy.

ANTONI ROIG BATALLA – Full Professor of Constitutional Law, Universitat Autònoma de Barcelona, Spain.

EYAL SABRO – Lawyer. Privacy consultant & DPO, University of Cordoba, Spain.

ANDREA SENATORE – Postdoctoral Research Fellow, Università degli Studi di Salerno Italy.

ANDREA TARAMELLI – Full Professor of Geografy, IUSS Pavia, Italy.

BARTOLOMÉ TORRALBO MUÑOZ – Assistant Professor, University of Cordoba, Spain. Ph.D. in Criminal Law, University of Cordoba, Spain.

LAURA VALLE – Associate Professor of Private Law, Libera Università di Bolzano, Italy.