ISSN: 2704-8012

SUOR ORSOLA BENINCASA
UNIVERSITÀ EDITRICE

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu



2024/2

EJPLT
ISSN: 2704-8012

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2024/2

SUOR ORSOLA BENINCASA
UNIVERSITÀ EDITRICE

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

Co-funded by the European Union

*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), 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) (611876-EPP-1-2019-1-IT-EPPJMO-CHAIR).

In 2022 EJPLT has been further implemented thanks to winning the co-funding for the Jean Monnet Chair project 'European Green Rights: reshaping fundamental rights for next generations' (EUGREENEXT) (ERASMUS-JMO-2021-HEI-TCH-RSCH).

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*

Indexed in

www.ejplt.tatodpr.eu ejplt@unisob.na.it

https://doi.org/10.57230/EJPLT
https://doi.org/10.57230/EJPLT242

Editing Luciana Trama

Design Flavia Soprani

Development Maria Teresa Lo Conte

© Copyright 2024 by Suor Orsola Benincasa Università Editrice, published in December 2024
ISSN: 2704-8012
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

EJPLT
ISSN: 2704-8012

EDITOR IN CHIEF/DIRECTOR
Prof. Avv. Lucilla Gatt – Università degli Studi Suor Orsola Benincasa di Napoli, Italy

VICE-DIRECTOR
Prof. Ilaria Amelia 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

ADVISOR BOARD – SCIENTIFIC COMMITTEE
Prof. Pasquale Arpaia – Università degli Studi di Napoli Federico II, Italy
Prof. Giovanna Capilli – Università San Raffaele di Roma, Italy
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. Roberto Montanari – Università degli Studi Suor Orsola Benincasa, Italy
Prof. Roberta Montinaro – Università degli Studi di Napoli l'Orientale, Italy
Prof. Andrew Morris – University of Loughborough, United Kingdom
Prof. Juan Pablo Murga Fernandez – Universidad de Sevilla, Spain
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. Jaime Alcalde Silva – Pontificia Universidad Católica de Chile, Chile
Prof. Jeremy Antippas – Université de Bretagne Sud, France
Prof. Miguel Álvarez Ortega – Kyoto University, Japan, and Universidad de Sevilla, Spain
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. Carlos Antonio Agurto Gonzáles – Universidad Nacional Mayor de San Marcos, Peru
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. Giuseppe Corasaniti – Universitas Mercatorum e Luiss, Italy
Prof. Gina Gioia – Università degli Studi della Tuscia, Italy
Prof. Alberto Giulio Cianci – Università degli Studi di Perugia, Italy
Prof. Maria Antonia Ciocia – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Valentina Vincenza Cuocci – Università di Foggia, Italy
Prof. Giovanna D'Alfonso – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Giuseppe Di Vetta – Scuola Universitaria Superiore Sant'Anna di Pisa, Italy
Prof. Carlos de Cores Helguera – Universidad CLAEH del Uruguay, Uruguay
Prof. Manuel Espejo Lerdo de Tejada – Universidad de Sevilla, Spain
Prof. Elżbieta Feret – Uniwersytet Rzeszowski, Poland
Prof. Marco Giacalone – Vrije Universiteit Brussel, Belgium
Prof. Giovanni Iorio – Università degli Studi di Milano Bicocca, Italy
Prof. Arndt Künnecke – Hochschule des Bundes für öffentliche Verwaltung, Germany
Prof. Leysser Luggi Leon Hilario– Pontificia Universidad Católica del Perú
Prof. Martin Maguire – University of Loughborough, United Kingdom
Prof. Paola Manes – Alma Mater Studiorum Università di Bologna, Italy

European Journal of Privacy Law & Technologies

EJPLT
ISSN: 2704-8012

Prof. Giovanni Martini – Università degli Studi della Campania Luigi Vanvitelli, 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. Nora Ni Loideain – Institute of Advanced Legal Studies of London, United Kingdom
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. Julio Álvarez Rubio – Universidad de Cantabria Santander, Spain
Prof. Gemma Rubio – Universitat de Barcelona, Spain
Prof. Carla Solinas – Università degli Studi di Roma Tor Vergata, Italy
Prof. Avv. Laura Valle – Libera Università di Bolzano, Italy
Prof. Isabel Zurita Martin – Universidad de Cádiz, Spain
Prof. Lihong Zhang – East University of Political Science and Law, Shanghai, China

MEMBERS OF THE EDITORIAL BOARD
Prof. Sara Lorenzo Cabrera – Universidad de La Laguna, Spain
Prof. Manuel Pereiro Càrceles – University of Valencia, 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. Ranieri Razzante – Università degli Studi di Bologna, Italy
Prof. Avv. Alessandra Sardu – Università degli Studi di Modena e Reggio Emilia, Italy
Prof. Sara Tommasi – Università del Salento, Italy
Ph.D. Avv. Mark Giancaspro – University of Adelaide, Australia
Prof. Hakeem Yusuf – University of Derby, United Kingdom
Ph.D. Avv. Livia Aulino – Università degli Studi di Napoli Federico II, Italy
Ph.D. Avv. Andrea D'Alessio – Università degli Studi di Teramo, 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 – 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 – Universität Luzern, Switzerland
Ph.D. Sara Saleri – Alma Mater Studiorum Università di Bologna, Italy
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) Davide D'Aloia – Università degli Studi Suor Orsola Benincasa, Italy
Ph.D. (c) Alessandra Fabrocini – Sapienza Università di Roma, Italy
Ph.D. (c) Gabriela García Vera – Uniwersytet Rzeszowski, Poland
Ph.D. Emanuele Garzia – Università Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Simona Ghionzoli – Università degli Studi di Napoli l'Orientale, Italy
Ph.D. (c) Pablo Guédon – Université Jean Moulin Lyon 3, France
Ph.D. (c) Luigi Izzo – Università degli Studi Suor Orsola Benincasa, Italy
Ph.D. (c) Marie Potus – Université Jean Moulin Lyon 3, France
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



Summary

pp.

Editorial

Digital bioethics... Next step forward? | Bioetica digitale... Il prossimo passo in avanti? *10*
Giuseppe Corasaniti

Articles

Tre appunti in materia di sostenibilità, welfare e Bauhaus europeo | Three notes on sustainability, welfare and the European Bauhaus *19*
Manolita Francesca

La tutela dei dati biometrici tra GDPR e AI ACT | The protection of biometric data between the GDPR and the AI ACT *37*
Anna Carla Nazzaro

Plataformas digitales y derechos de la personalidad | Digital platforms and personality rights *54*
Fernando Carbajo Cascón

Artificial intelligence and infringement of intellectual property | Intelligenza artificiale e violazione della proprietà intellettuale *84*
Luca Nivarra

I «Registri delle attività di trattamento» tra responsabilizzazione e presupposto di liceità del trattamento dei dati personali | «Records of processing activities» between accountability and the prerequisite of lawfulness of personal data processing *102*
Davide Achille

L'identità personale dei minori, tra responsabilità genitoriale e capacità di autodeterminarsi | The personal identity of minors, between parental responsibility and the capacity for self-determination *115*
Caterina Murgo

Animals and Nature in Buddhism: From Normative Sources to Contemporary Environmentalism | Animali e Natura nel Buddhismo: dalle fonti normative all'ambientalismo contemporaneo *129*
Miguel Álvarez Ortega

Intelligenza artificiale sostenibile e tutela dei green rights | Sustainable artificial intelligence and the protection of green rights *147*
Maria Cristina Gaeta

Civil liability regimes for AI-related torts within the Italian legal system | I criteri di imputazione della responsabilità civile per i danni cagionati dall'IA nell'ordinamento giuridico italiano *172*
Tommaso De Mari Casareto dal Verme

Focus

FRIA implementation model according to the AI Act | Modello di attuazione FRIA in applicazione dell'AI Act *192*
Lucilla Gatt, Ilaria Amelia Caggiano, Maria Cristina Gaeta, Emiliano Troisi, Roberta Savella, Roberto Trasarti, Francesca Pratesi

Admissibility of Illegally obtained e-evidence: A critical study of EU law and the Precedents of the European Court of Human Rights | Ammissibilità delle prove elettroniche ottenute illegalmente: uno studio critico del diritto dell'UE e dei precedenti della Corte europea dei diritti dell'uomo *205*
Oleksii Volodymyrovych Kostenko, Vahid Akefi Ghazian

Meta-analysis of privacy legal framework: revising the various approaches for balancing privacy risks and usability of healthcare information systems | Meta-analisi del quadro normativo sulla privacy: revisione dei differenti approcci per bilanciare i rischi per la privacy e l'usabilità dei sistemi informativi sanitari *221*
Matjaž Drev, Dalibor Stanimirović, Boštjan Delak

Neurotechnology in the research of evidence and in decision-making process: a dual perspective analysis | Le neurotecnologie nella ricerca della prova e nei processi decisori: un'analisi a doppia prospettiva *233*
Alice Angelini

Plataforma europea de Resolución de Litigios en Línea (RLL): ecosistema digital en vía de extinción | European Online Dispute Resolution Platform (ODP): digital ecosystem on the verge of extinction *247*
Juan Sebastián Alejandro Perilla Granados

List of author *261*

SECTION I
EDITORIAL

Corasaniti G, 'Digital bioethics... Next step forward? ' (2024) 2 EJPLT, 10 – 17.
DOI: https://doi.org/10.57230/EJPLT242GC

EJPLT
ISSN 2704-8012



Digital bioethics... Next step forward?

Bioetica digitale... Il prossimo passo in avanti?

GIUSEPPE CORASANITI
Full Professor of Philosophy of Digital Law
Universitas Mercatorum
Full Professor of Artificial Intelligence and Law
LUISS Guido Carli

Abstract

The integration of artificial intelligence (AI) in healthcare raises ethical and legal challenges, requiring a strong regulatory framework. The WHO emphasises autonomy, transparency and accountability in the use of AI, while the EU regulation classifies medical AI as high-risk, imposing compliance and data protection obligations. Liability remains a key issue due to AI's opaque decision-making processes. Digital bioethics highlights the need for interdisciplinary collaboration to ensure equitable access, mitigate bias, and balance technological advances with patient rights and legal responsibilities. A holistic approach is essential for the ethical integration of AI in medicine.

L'integrazione dell'intelligenza artificiale (IA) nell'assistenza sanitaria solleva sfide etiche e legali, richiedendo un solido quadro normativo. L'OMS pone l'accento sull'autonomia, la trasparenza e la responsabilità nell'uso dell'IA, mentre il regolamento dell'UE classifica l'IA medica come ad alto rischio, imponendo obblighi di conformità e protezione dei dati. La responsabilità rimane una questione fondamentale a causa dell'opacità dei processi decisionali dell'IA. La bioetica digitale evidenzia la necessità di una collaborazione interdisciplinare per garantire un accesso equo, attenuare i pregiudizi e bilanciare i progressi tecnologici con i diritti dei pazienti e le responsabilità legali. Un approccio olistico è essenziale per l'integrazione etica dell'IA in medicina.

© The author(s) 2024, 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; Healthcare; Digital Bioetchics

Summary: 1. Introduction. – 2. Regulatory Framework for AI in Healthcare. – 3. Liability and Ethical Considerations in AI-driven Healthcare. – 4. Digital Bioethics and the Ethical Use of AI in Healthcare. – 5. Conclusions.

1. Introduction.

The World Health Organization (WHO) has published guidance on the ethical use of artificial intelligence (AI) in healthcare. According to the WHO, AI holds great promise for improving healthcare worldwide if ethics and human rights are at the heart of its design, implementation, and use. To regulate and govern AI, the WHO has published new guidance that provides six principles for limiting risks and maximizing the inherent opportunities of AI for health. These principles are essentially indicated in the need to protect the autonomy of operators, in the promotion of people's safety and well-being, but also in the promotion of transparency and responsibility through ethically correct and transparent choices through reactive and sustainable tools. The report also highlights that opportunities are linked to challenges and risks, including the unethical collection and use of health data; encoded biases in algorithms and AI risks for patient safety, cybersecurity and the environment. By following these underlying principles and addressing these general issues, we can understand that ensuring the ethical use of AI in healthcare. In the hospital environment, it means stimulating the responsible use of machinery and diagnostic software that replace the professional operator, and it is increasingly common for artificial intelligence systems to intervene in the treatment process both in the diagnostic and therapeutic phases, allowing the healthcare worker to reach more certain and precise diagnoses and more effective and less invasive surgical therapies.

2. Regulatory Framework for AI in Healthcare.

The upcoming European regulation on artificial intelligence specifically addresses the issue of medical and health applications in different ways, depending on the level of risk they pose. In general, the proposed regulation sets out requirements and obligations for developers, providers and users of artificial intelligence systems operating in the EU, in order to ensure security, transparency, traceability, non-discrimination and respect for the privacy and fundamental rights of individuals.

In particular, medical and health applications are considered high-risk if they fall into one of the following categories such as medical devices or health products that are or incorporate artificial intelligence systems, such as those used for the diagnosis, prognosis, monitoring or treatment of physical or mental diseases or conditions, intelligent systems that provide essential social services, such as those used for remote healthcare, medical emergency

management or care for the elderly or disabled and those that are then used for remote biometric identification, such as those used for facial or fingerprint recognition.

For these high-risk applications, the proposed regulation provides that: Artificial intelligence systems are subject to a conformity assessment before being placed on the market or put into service, in order to verify compliance with the requirements of the regulation and are provided with clear and complete information on their characteristics, functionality and limitations, as well as instructions for their correct and ethical use.

They will have to be equipped with specific tools to ensure the quality and security of the data used for their learning and operation, as well as to prevent or mitigate the risks of bias or discrimination. In addition, they will in any case have to ensure the traceability and documentation of their operations and their results, as well as to facilitate human control and human intervention in case of need and respect for the privacy and protection of the personal health data of users and those affected by their decisions or actions. Finally, providers and users of AI systems register their systems in a European AI database, in order to facilitate monitoring and supervision by competent authorities.

3. Liability and Ethical Considerations in AI-driven Healthcare.

Even in the absence of a precise regulatory discipline, the risk of easily incurring civil or criminal liability is evident for the health care provider. One of the main problems already addressed is the very nature of the tool, which sometimes does not allow the operator to access the processes through which the desired result is achieved. And this profile is extremely delicate if and to the extent that the system has been provided with adequate operating instructions and if and to the extent that these instructions have been complete and subject to adequate training at the health and internal level.

This system has already been problematically defined by legal doctrine, noting that it is not always possible for man and in particular for the operator of a health profession to know and verify the logical process and the motivation of the machine's choices. When considering the civil liability of the doctor and the hospital, this means that the non-contractual liability of the doctor, as it is currently regulated by law, would require the injured party to provide almost difficult evidence to obtain compensation for damage to health caused by the doctor using AI tools, due to the opaque nature of the tool used by the doctor, which does not allow an easy identification of a causal link between fact and damage. The use of artificial intelligence in health services allows the doctor to monitor and confirm the outcome produced by the program. This is because the doctor is tasked with guiding the algorithm in real-time and because there is an opportunity to review the software's output. This moment of verification allows the doctor to correct any errors before the treatment is administered to the patient.

When software works with a high level of autonomy, intervening directly on the patient for diagnostic or therapeutic purposes, the question of liability becomes more complex. This is especially true for software that, due to its

design and development, does not allow you to clearly understand how it works.

In such circumstances, it is important to determine whether the physician can be held liable for the damage caused by the algorithm, even if he or she does not have the real possibility of influencing or correcting the actions of the software. In fact, possible malfunctions and related damage to patients cannot be ruled out, especially since artificial intelligence systems, especially generative ones, are subject to evolutions, updates and changes that affect their operation, often in an unpredictable way for developers.

In addition, it is crucial to consider that the continuous evolution of artificial intelligence could lead to future scenarios in which the software could make independent and even original and innovative clinical decisions in the solution of the clinical or surgical problem. In these cases, the question of responsibility becomes even more critical. New regulatory frameworks may need to be developed to address these emerging challenges and ensure patient safety.

The evidentiary aspect, however, does not appear to be so decisive if the same principle of reversal of the burden of proof were to be adopted for the regulation of artificial intelligence as is currently provided for in the processing of personal data, on the basis of the perspectives gained at European level. In any case, there are still margins of irresponsibility for robots and in any case for algorithmic solutions embedded in the hardware, which then means that the social cost of the damage could eventually fall on the injured party. There is still no shortage of analyses aimed at the preliminary identification of viable legal solutions is considered of considerable urgency if we think of the growth and spread of the use of AI systems in recent years, in all sectors and in particular in the health sector, and if it is assumed that an increase in the use of the medium even in the short term will lead, in the short term, an inevitable increase in the chances that a harmful event will result from the use of the vehicle. It is not possible to conceive regulatory and ethical solutions except in an interdisciplinary key to ensure a balanced and equitable development of smart technologies in health Already in a 2017 Resolution, the European Parliament hypothesizes the alternative introduction of an objective liability regime or a risk management approach, which makes it possible to verify which is the subject who "is able to minimize the risks and deal with the negative impact".

Solutions that, according to some, are not to be envisaged as alternatives, but rather as reconcilable with each other, both forfeitable in a system of protection that works in a uniform manner.

And in fact, it is certain that the choice of an objective protection system does not in any way exclude, and indeed in some ways suggests, the possibility of providing rules aimed at risk management by subjects operating along the production chain. But who could be responsible for mistakes or malicious decisions made by AI systems? How to define a concept of responsibility in every case in which the diagnostic or therapeutic decision is taken by an algorithm?

In principle, a responsibility can be defined from the point of view of the design of the system or the incorrect setting of the criteria of its operation, but much more complex appears to be the issue that refers to the synchronization of data, the adequate training and training of the personnel in charge, the

adequate understanding of what is the operational functioning of the artificial intelligence system provided on the basis of precise or imprecise settings, which could clearly be an element that can be evaluated differently depending on the contexts and characters of the system itself.

A first problem concerns in particular what is the training of the data and the verification of the completeness and correctness of the datasets themselves. In fact, there has been the possibility that AI in all fields of its application perpetuates or amplifies existing discriminations. Hence the need to address bias in training. In fact, algorithms often operate as real "black boxes", difficult to control and also difficult to reconstruct in options as well as in acquisitions from structured datasets, but the transparency of decision-making methods should also be highlighted according to criteria that are always transparent and explainable. The need to structure the specific sector regulations in the health and pharmaceutical sectors also emerges in the health sector.

Many software can be classified as medical devices according to Regulation (EU) 2017/745, but this regulation does not provide indications on liability, limiting itself to providing for a general liability of the manufacturer in any possible case of malfunctions and damages resulting from the same, with the attached obligation to ensure sufficient financial coverage in relation to this liability, typically in the form of insurance. Furthermore, it is quite evident that a very delicate evidentiary issue is specifically framed for the injured party, who may not be able to demonstrate not only a malfunction of the apparatus but also its functional non-compliance with the adequate resolution deriving from an incorrect reference data context.

4. Digital Bioethics and the Ethical Use of AI in Healthcare.

A digital "bioethics" is therefore envisaged in which, beyond the priority evaluations of a moral order, the criteria can be precisely verified in a synergistic and interactive key through feedback and information strategies not limited to the traditional fields of medical sciences, but extended in the professional comparison and in the cognitive contribution of other categories involved to encourage an increasingly careful use of digital tools. Digital bioethics can therefore be defined as an emerging discipline that deals with the ethical issues raised by the use of digital technologies in the field of health, life and society.

The issue of digital bioethics is then divided into several aspects that can be variously explored, including first of all the effective protection of the personal and sensitive data of patients and citizens, which can be collected, processed and shared by digital devices, applications and platforms, often without their informed consent or with the risk of privacy and security violations. In addition, in general, from a health point of view, the issue of equitable and universal access to digital health resources and services arises, which can offer opportunities for prevention, diagnosis, treatment and monitoring, but also create disparities and discrimination between those who have them and those who are excluded or marginalized. The same varied responsibility and transparency of algorithms and artificial intelligence presents controversial

aspects that can influence clinical decisions, health policies and the behavior of those involved in the health system, but also generate errors, biases and biases that can compromise the quality and effectiveness of care and the protection of patients' rights. There is general agreement on the issue of safeguarding the dignity and autonomy of people, who may be subjected to forms of surveillance, manipulation or coercion by public or private actors who use digital technologies to control, influence or modify their choices, values and identities.

Digital bioethics therefore increasingly requires a multidisciplinary and participatory approach, involving all interested stakeholders (health professionals, researchers, developers, regulators, patients, citizens) in dialogue, reflection and the definition of principles, norms and good practices for an ethical, responsible and sustainable use of digital technologies in the field of health, life and society. It should be based on a multidisciplinary and participatory approach, involving experts from different areas of knowledge, stakeholders, users and citizens.

Therefore, digital bioethics must overcome an individualistic view and focus on the interconnections and interdependencies between humans and technology. This requires an interdisciplinary approach involving different skills to address the ethical challenges posed by the use of algorithms, big data and artificial intelligence in the medical and healthcare fields. Only through a broad and shared ethical reflection accessible to all, classical bioethics will be able to evolve and will be able to give a meaning and a valuable orientation to techno-scientific progress, avoiding its "dehumanization".

5. Conclusions.

New issues are envisaged such as the essentiality of treatments in relation to their cost in terms of access to intelligent technologies, and the traditional responsibility of the professional seems to have to be extended in many cases in the consideration of the understanding of the different techniques of interpretation of the available data, of the opportunity to know how to read and interpret diagnostic data in the light of what is expected to be the best technology in relation to the case diagnostic test in the light of a medium interpretation as well as in consideration of the resources available to the health facility concerned.

It is no longer possible to conceive of a role of ethics understood in an integrative sense, having instead to conceive of a growing integration between different experiences, each oriented towards the well-being and recovery of the patient but at the same time each one that can be connected to the best available technology, to the ability to connect and compare with the outside world for the health facility in order to verify not only the possible options but above all in a collective way to reconnect the picture information available in an increasingly globalized context.

The same organization, typical of traditional bioethics committees, which are mostly based on a comparison of experiences, each understood in its separateness, could require an adjustment in the sense of expanding digital

sensitivity and informed attention to emerging technologies. Today more than ever in the context of healthcare facilities it is necessary to proceed with the articulation of a coordinated series of controls that are oriented in a sensitive and innovative way towards a dimension of recovery and well-being that cannot fail to be considered except in the digital sphere. All this does not integrate only one problem but rather describes a growing series of adaptive problems that concern both strictly and traditionally legal issues as well as the need to understand as soon as possible through technologies what is the best choice in terms of effective protection of citizens' right to health and at the same time the meaning and overall orientation of the information available in terms of therapy and therapeutic intervention through the best technologies.

All this requires a constant exchange of information between public and private, a consideration and classification of data and aggregation of data in homogeneous terms and is in some way organic with respect to what is the main function of health facilities. In my opinion, it is necessary to maintain an open and above all sensitive vision, capable of being able to read what the data express in their direct incidence in statistical terms but above all what the data do not express, that is, what is usually traced back to the onset of pathologies applied not considered and to forms of therapy and diagnosis, even of an experimental nature, based on the correct way of associating emerging patterns of a specialized nature, all the more so in a context globalized.

The challenges that await the law of medical sciences can be understood and interpreted through a continuous comparison, a sensitivity and a constant openness to technological knowledge that is not only an uncritical use, but contrary to the use of the human being. thus improving their condition as well as their expectations of well-being and recovery.

A first problematic aspect is represented by the need to ensure an integrated and complementary vision in bioethical terms, and this passes through an integrated and complementary vision of the available technologies, a careful reading of the data and alternatives that can be traced and defined in terms of treatment and medical intervention, this passes through a new organization of the competences usually associated with bioethics committees, in which knowledge does not intersect, but in some way remains separate, defining only an optimal conception following a central point of view which is the health one, indeed mostly the one specialized in medical terms, without sometimes glimpsing the usefulness of a comparative method or an applicative vision of the technology available and usable in the concrete scenario. Just as it was decided not to leave doctors alone in the crucial choices relating to health management and the optimal organization of services, today it seems essential to understand how technologies can simplify and integrate the communication framework but also define new protocols and therapeutic systems through a constant, open discussion defined in an open sharing action that can be linked to different areas and evolutionary scenarios that were previously unrelated to the past.

Digital technologies integrate and integrate with each other and require a sensitive, conscious and aware vision of what are the possible areas of risk, but equally capable of asking questions about the methods generally practiced and of following new and original paths never considered, in a constant research

that knows how to understand and define new possible paths[i].

[i] T Magnin, P. Giorgini, 'Digital Driven Technosciences: Epistemological and Ethical Questioning' (2022) 1 Etica & politica - Ethics & politics, 379; G Di Rosa, 'Quali regole per i sistemi automatizzati "intelligenti"?' (2021) 5 Rivista di diritto civile, 823; L Palazzani, 'Clinical trials in the time of a pandemic: implications for informed consent' (2021) 2s BioLaw Journal - Rivista di BioDiritto, 35; C Botrugno, 'Innovazione tecnologica in salute e "commodification". Verso un nuovo dovere di protezione dell'individuo?' (2020) 1 Jura Gentium, 140; G Fioriglio, *Informatica medica e diritto. Un'introduzione* (Mucchi Editore 2020); A D'Aloia, 'Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale' (2019) 1 BioLaw Journal - Rivista di BioDiritto, 1; EA Ferioli, 'L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel "welfare" italiano' (2019) 1 BioLaw Journal - Rivista di BioDiritto, 10; L Marilotti, 'Ipotesi per una gestione partecipata delle biobanche genetiche concepite come beni comuni' (2023) 2 BioLaw Journal - Rivista di BioDiritto, 383; G Fioriglio, 'Intelligenza artificiale e medicina: alcune riflessioni sui profili giuridici ed etici' (2021) 143 Notizie di Politeia, 162-166; MD Garasic, 'Informed consent, clinical research, covid-19 and contact tracing apps: some neuroethical concerns' (2021) 2s BioLaw Journal - Rivista di BioDiritto, 85; A Santosuosso, 'About coevolution of humans and intelligent machines: Preliminary notes' (2021) 1s BioLaw Journal - Rivista di BioDiritto, 445; A Monreale, 'Rischi etico-legali dell'Intelligenza Artificiale' (2020) 3 DPCE online, 3391; FG Pizzetti, 'La Costituzione e l'uso in sede giudiziaria delle neuroscienze (e dell'intelligenza artificiale): spunti di riflessione' (2019) 2s BioLaw Journal - Rivista di BioDiritto, 697; C Casonato, 'Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro' (2019) 2s BioLaw Journal - Rivista di BioDiritto, 711; D Amoroso, G Tamburrini, 'I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?' (2019) 1 BioLaw Journal - Rivista di BioDiritto, 2; S Marchiori, P Sommaggio, 'Break the chains: a new way to consider machine's moral problems' (2018) 3 BioLaw Journal - Rivista di BioDiritto, 15; A Bertolini, 'Human-Robot Interaction and Deception' (2018) 2 Osservatorio del diritto civile e commerciale, 645; N Busto, 'Carta europea sulla robotica: una proposta di "roboethics" per le "self-driving car"' (2017) 2 Ciberspazio e Diritto, 289; EM Biganzoli, B Cesara, 'La figura del biostatistico nei Comitati Etici (CE). Linee guida per il ruolo del biostatistico e per l'attività del biostatistico nella revisione dei protocolli degli studi proposti al parere dei CE' (2016) 5 Medicina e morale, 567; C Salazar, 'Umano, troppo umano...o no? Robot, androidi e cyborg nel "mondo del diritto" (prime notazioni)' (2014) 1 BioLaw Journal - Rivista di BioDiritto, 12; L Caenazzo, D Rodriguez, P Tozzo, 'Aspetti etici e tutela dei minori nella gestione delle biobanche a scopo di ricerca e forense in Italia' (2011) 2-3 Zacchia, 237; A Marturano, 'Biologi molecolari: hacker di dati umani? Bioetica e proprietà intellettuale nella ricerca bioinformatica' (2006) 4 Medicina e morale, 741.

SECTION II
ARTICLES

Francesca M, 'Tre appunti in materia di sostenibilità, welfare e Bauhaus europeo' (2024) 2 EJPLT, 19 – 36.
DOI: https://doi.org/10.57230/EJPLT242FM

EJPLT
ISSN 2704-8012



Tre appunti in materia di sostenibilità, welfare e Bauhaus europeo

Three notes on sustainability, welfare and the European Bauhaus

MANOLITA FRANCESCA
Professore ordinario di Diritto privato
Università degli Studi di Foggia

Abstract

Il lavoro offre un ritratto a tinte fosche del governo della sostenibilità e dei suoi costi. Gli effetti sull'economia fondamentale delle politiche macroeconomiche vengono analizzati in tre settori cruciali: immobiliare, finanziario ed energetico. L'analisi restituisce la sensazione che Sostenibilità e *Welfare* siano misure direttamente proporzionali, l'aumento del primo fattore accentua la divaricazione reddituale alla base delle azioni di *Welfare*.

The paper offers a dark portrait of sustainability governance and its costs. The effects on the fundamental economy of macroeconomic policies are analysed in three crucial areas: real estate, finance and energy. The analysis gives the impression that Sustainability and Welfare are directly proportional measures, the increase of the first factor accentuates the income gap underlying Welfare actions.

* Il lavoro riproduce, con alcune revisioni e integrazioni, parte del testo della relazione svolta nell'Aula consiliare, Consiglio Regionale Puglia, Via Giovanni Gentile, 52, Bari, in occasione del Convegno "L'altra faccia del welfare. Azione pubblica, rapporti privati e impatti disfunzionali", organizzato il 4 luglio 2024, nell'ambito delle attività del progetto di collaborazione tra Consiglio regionale della Puglia ed Università di Foggia – Dipartimento di Scienze Sociali "Analisi e supporto alle politiche pubbliche in materia di Diritti e Libertà, Welfare sussidiario, Transizione ecologica e Finanza sostenibile".

© The author(s) 2024, 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; Green deal europeo; ESG; ADR; energia; welfare

Summary: 1. Premessa dell'indagine: governo della sostenibilità e politiche di welfare. – 2. Settore immobiliare e sostenibilità. – 3. Settore finanziario e sostenibilità. – 4. Settore energetico e sostenibilità.

1. Premessa dell'indagine: governo della sostenibilità e politiche di welfare.

Welfare e Sostenibilità sono ormai espressioni della cultura *mainstream*, invocate come obiettivi macroeconomici paralleli o semplicemente non collidenti. Eppure, i due termini costituiscono due facce della stessa medaglia, anzi – si potrebbe osservare – il *Welfare* rappresenta il costo della Sostenibilità.

Là dove si volesse cercare una rappresentazione o una immagine di quanto si afferma, la si troverebbe nella *Relatività* di Escher. I diversi orientamenti gravitazionali percorsi da esseri tutto sommato simili ci consegnano una prospettiva di instabilità, di vertigine prodotta da spinte opposte. È il mondo che si proverà a descrivere in questo lavoro, là dove gli illustri protagonisti (Sostenibilità e Welfare) sono espressione di spinte autonome e che tuttavia costringono gli anonimi componenti della società a continui percorsi e riposizionamenti.

La sensazione è che Sostenibilità e Welfare siano misure direttamente proporzionali, l'aumento del primo fattore accentua la divaricazione reddituale alla base delle azioni di Welfare[1].

Quella sensazione diventa qualcosa in più in tre emblematici settori dove si assiste più che altrove a una sostenibilità applicata (*rectius*: a un governo della sostenibilità).

2. Settore immobiliare e sostenibilità.

Nel tempo la pressione fiscale sugli immobili ha assunto un nuovo impatto, con una funzione di ausilio a obiettivi energetici, ambientali e sociali[2]. Il paio è rintracciabile nelle linee di intervento fornite dall'OCSE, nello studio economico del 2023 sull'Italia, circa la necessità di adoperarsi sulla politica fiscale, in particolare immobiliare. Qui si afferma, a proposito delle politiche fiscali attese, che «lo spostamento dell'imposizione fiscale dal lavoro alla proprietà e ai consumi tutelerebbe il gettito fiscale del Paese e, al contempo, renderebbe il sistema più funzionale alla crescita».

[1] Le applicazioni sfuggono al dover essere del concetto di sostenibilità. Lavoro, proprietà, impresa, obbligazioni, contratto, diventano "sostenibili" laddove assicurino a tutti il minimo vitale dello *status personae*, così E. CATERINI, *Sostenibilità e ordinamento civile. Per una riproposizione della questione sociale*, Napoli, 2018, p. 26. In merito v. anche ID., *Il principio di sostenibilità nel diritto civil-costituzionale delle nuove tecnologie*, Convegno, *Il principio di sostenibilità: fonti, contenuto e funzioni*, Parma,17 e 18 ottobre 2024, qui l'a. afferma che la «sostenibilità è una particolare espressione dei princìpi di solidarietà e uguaglianza, una speciale composizione che varia al variare delle condizioni personali».

[2] In merito, sia consentito un rinvio a M. FRANCESCA, *Ieri, oggi, domani: note introduttive sullo stato della proprietà immobiliare*, in M. FRANCESCA e L. FOLLIERI (a cura di), *Rinuncia alla proprietà immobiliare. Discussione intorno all'ammissibilità dell'atto e alle soluzioni alternative*, Napoli, 2024, pp. 11 ss.

La questione non è nuova. Gli immobili assumono una funzione centrale in molte azioni, prima tra tutte nella partita della sostenibilità energetica. È sufficiente richiamare l'art. 1, comma 1, d.lgs. 19 agosto 2005, n. 192, che in attuazione della direttiva 2002/91/CE relativa al rendimento energetico nell'edilizia, ha stabilito criteri, condizioni e modalità «per migliorare le prestazioni energetiche degli edifici al fine di favorire lo sviluppo, la valorizzazione e l'integrazione delle fonti rinnovabili e la diversificazione energetica, contribuire a conseguire gli obiettivi nazionali di limitazione delle emissioni di gas a effetto serra posti dal protocollo di Kyoto, promuovere la competitività dei comparti più avanzati attraverso lo sviluppo tecnologico».

Qui viene affidato allo Stato, alle regioni e alle province autonome un ruolo di sorveglianza, attuazione e promozione «dell'uso razionale dell'energia e delle fonti rinnovabili, anche attraverso la sensibilizzazione e l'informazione degli utenti finali» (art. 1, comma 3), e si introduce il c.d. certificato APE. L'attestato di certificazione energetica o di rendimento energetico degli edifici è funzionale ad attestare e conseguentemente classificare gli immobili in ragione della prestazione energetica. Esso è diventato obbligatorio dal 1° luglio 2009 in tutti i casi di compravendita degli immobili e dal 1° luglio 2010 è altresì obbligatorio in caso di locazioni e di operazioni di surroga nei contratti di mutuo, quest'ultima necessaria in caso di spostamento della propria esposizione debitoria ad altra banca.

Banca d'Italia in uno studio dal titolo *"The capitalization of Energy Labels into House Price. Evidence from Italy"*[3] ha dimostrato come il livello di classificazione energetica impatti sul prezzo degli immobili per il 25% a parità di altre condizioni. Sebbene ciò dipenda dal clima locale delle province analizzate, è evidente che le esigenze della transizione energetica hanno determinato una congerie di azioni positive volte a incidere sulla tenuta degli immobili.

Insomma: i titolari di immobili, a prescindere dalla volontà di partecipare a interventi di impatto sistematico, vedono i propri beni assumere il ruolo di strumenti di politiche di impatto sociale e ambientale[4].

Questi non si definiscono ESG – nomenclatura propria del sistema finanziario con la quale si indicano le partite di titoli caricati di interventi a impatto sociale e ambientale – eppure somigliano molto[5].

---

[3] M. LOBERTO, A. MISTRETTA e M. SPURI, *The capitalization of energy labels into house prices. Evidence from Italy*, in *Questioni di Economia e Finanza (Occasional Papers)*, n. 818, novembre 2023.

[4] In merito v. le lucide considerazioni di F. ADDIS, *Rinuncia alla proprietà immobiliare. Considerazioni a margine di un Convegno*, in M. FRANCESCA e L. FOLLIERI (a cura di), *Rinuncia alla proprietà immobiliare*, cit., pp. 127 ss.: «Non credo che vada incoraggiata la tendenza a stigmatizzare la natura egoistica di scelte dismissive. Quando esse maturano, dimostrano pur sempre uno stato di difficoltà economica che induce a comportamenti che sovvertono quello che potrebbe essere considerato l'ordine naturale dell'umana inclinazione all'appropriazione. Se un privato non è in grado di sostenere i costi di gestione di un bene o non è nelle condizioni di affrontare i rischi derivanti dalla pericolosità di un bene, ciò rappresenta – di per sé – un problema che valica la dimensione privata e finirà quasi inevitabilmente per trasformarsi in una questione di rilievo pubblico.
D'altra parte, mi pare miope e infruttuosa un'impostazione del problema che muova da una rigida affermazione dell'esigenza di controllo e limitazione della spesa pubblica».

[5] È molto più di una somiglianza. Il *Final Report on Social Taxonomi, Platform on Sustainable Finance*, February 2022 e il Parere del Comitato economico e sociale europeo sul tema: «Tassonomia sociale – Sfide e opportunità» (2022/C 486/03) includono le esigenze legate all'economia fondamentale e, tra queste, quelle abitative nell'area degli obiettivi finanziari connessi alla sostenibilità sociale: «*Activities in these sectors certainly contribute to adequate living conditions. Nevertheless, it must be ensured that any criteria and indicators drawn up serve the purpose of directing capital flows to where they are needed*» (p. 51).

Le riferite considerazioni forniscono una chiave di lettura anche delle decisioni della Cassazione che qualificano la TARI quale prestazione doverosa a prescindere dalla concreta produzione di rifiuti; quest'ultima ormai reputata dovuta anche in caso di seconde case disabitate e senza utenze domestiche. Si discorre così di «una forte impronta pubblicistica»[6] e di assenza di sinallagma nella imposizione tributaria che tradisce lo specchio di azione di una misura ambientale.

In questo quadro, un medesimo bene – ad esempio acquisito per via ereditaria – spesso costituisce per il privato, che non ha condizioni particolarmente agiate, un peso economico rilevante – «*una proprietà insostenibile*»[7] – bisognoso quanto meno di una serie di interventi che lo rendano fruibile per la locazione o la vendita. Con buona probabilità è questo alla base del picco di rinunce alla proprietà immobiliare, che tuttavia trovano il limite dell'interesse pubblico a che il bene immobile resti presso il privato, quale strumento necessario per politiche ambientali, energetiche e sociali.

L'acquisto indiretto di un bene da parte dell'ente pubblico competente territorialmente *ex* art. 827 c.c., per effetto di una rinuncia abdicativa, aumenta le spese di gestione del settore pubblico con una forte incidenza sul vincolo di bilancio (di spesa)[8] del medesimo ente e parallelamente riduce le politiche di impatto perseguite per il tramite dell'effetto collettivo delle azioni individuali. E così accade che il potere abdicativo dei privati – a lungo espressione del potere assoluto dominicale – possa subire gli effetti di una nuova stagione delle politiche economiche al punto da essere ridotto o annullato ad opera di un erigendo contro-potere[9] di rifiuto riconosciuto alla Pubblica amministrazione[10].

Il 12 marzo 2024 il Parlamento europeo ha approvato la proposta di Direttiva europea sulle "Case *Green*"- Case Verdi[11]. L'obiettivo è noto: migliorare la classe energetica degli edifici entro precise scadenze e così ridurre il consumo

---

[6] Cass. civ., Sez. V, Ord. 20 giugno 2023, n. 17564, in *dejure.it*, in cui è ribadito il consolidato principio di diritto secondo cui «ai sensi della l. n. 147 del 2013, art. 1, comma 641, la TARI è dovuta, per la disponibilità dell'area produttrice di rifiuti e, dunque, unicamente per il fatto di occupare o detenere locali ed aree scoperte a qualsiasi uso adibiti; sono poi previste dai commi successivi deroghe, riduzioni di tariffe ed agevolazioni che operano in base a diversi presupposti di fatto e di diritto, di cui è onere del contribuente dedurre e provare la relativa sussistenza per vincere la presunzione di produttività di rifiuti posta dal suindicato comma 641. Anche la Tari, come la TARSU, è pertanto caratterizzata, indipendentemente dal *nomen iuris* utilizzato dalla normativa che la disciplina, da una struttura autoritativa e non sinallagmatica della prestazione, con la conseguente doverosità della prestazione, caratterizzata da una forte impronta pubblicistica». In merito v. le attente considerazioni di J. DE TULLIO, *Costituzione di un vincolo di uso pubblico su immobili diseconomici e regole di pubblicità*, in M. FRANCESCA e L. FOLLIERI (a cura di), *Rinuncia alla proprietà immobiliare*, cit., pp. 107 ss.

[7] La formulazione è di L. FOLLIERI, *La proprietà insostenibile. Rinuncia alla proprietà immobiliare tra interesse privato e ragioni della collettività*, Napoli, 2022.

[8] Discorre di «*traslazione* dei costi proprietari allo Stato» L. FOLLIERI, *o.u.c.*, pp. 45 ss.

[9] A quanto riferito si aggiungono – per la parte pubblica – gli effetti della verifica dei saldi strutturali ai fini della vendita/acquisto di beni immobili da parte della Pubblica amministrazione, stabilita dall'art. 12, comma 1, d.l. 6 luglio 2011, n. 98, convertito in l. 15 luglio 2011, n. 111, recante 'Disposizioni urgenti per la stabilizzazione finanziaria'. Quanto alla parte privata rinunciante si annidano i pericoli dell'abuso del diritto, sul punto v. L. FOLLIERI, *o.u.c.*, pp. 64 ss., nota 107.

[10] Sul punto ampiamente L. FOLLIERI, *o.u.c.*, pp. 185 ss. V. anche M. FRANCESCA e L. FOLLIERI (a cura di), *Rinuncia alla proprietà immobiliare*, cit. e, *ivi*, ampia documentazione.

[11] Ne fanno da sfondo le direttive UE, 11 dicembre 2018, n. 2002 sull'efficienza energetica e, 30 maggio 2018, n. 844 sulla prestazione energetica nell'edilizia. Entusiastica l'analisi di A. QUARANTA, *Nuova Direttiva sull'efficienza energetica: le prime impressioni a caldo*, in *Ambiente & sviluppo*, 2023, p. 731. Ricostruisce il quadro normativo e ne offre una interessante prospettiva nel rapporto con l'interesse abitativo F. OTTOMBRINO, *Interesse abitativo e circolazione immobiliare. Per una critica alla consumerizzazione del bene casa*, Napoli, 2024.

energetico e le emissioni prodotti nel settore edilizio attraverso una ristrutturazione "imposta" del patrimonio immobiliare.

Si chiama «neutralità climatica» la tappa da raggiungere entro il 2050 e si colloca nelle linee del percorso intrapreso con il Green Deal Europeo.

L'OICE (Associazione delle società di ingegneria e architettura di Confindustria) ha stimato che i costi potrebbero arrivare a 40.000/55.000 euro ad appartamento[12].

Nella Direttiva citata si parla di un nuovo *Bauhaus* europeo, già richiamato nella comunicazione della Commissione del 15 settembre 2021, nella descrizione di un'unica missione europea capace di coniugare bellezza e sostenibilità. La Direttiva del 2021 creava un rapporto stretto tra città intelligenti e impatto climatico e ancora nel 2024 si racconta che «L'iniziativa del nuovo *Bauhaus* europeo intende favorire una società più inclusiva che promuova il benessere di tutti in linea con il *Bauhaus* storico, che ha contribuito all'inclusione sociale e al benessere dei cittadini e, in particolare, delle comunità di lavoratori. Facilitando la formazione, la creazione di reti e fornendo orientamenti ad architetti, studenti, ingegneri e progettisti in base ai principi di sostenibilità, estetica e inclusione, l'iniziativa del nuovo *Bauhaus* europeo può consentire alle autorità locali di sviluppare soluzioni culturali e innovative per creare un ambiente edificato più sostenibile».

È evidente che si tratta di un nuovo obiettivo metaindividuale – che permea quelli dei singoli chiamati ad intervenire sulle proprie abitazioni – con il quale si tenta di combinare processi inclusivi con finalità di miglioramento climatico. È sintomatico che venga ambiziosamente richiamato il noto movimento architettonico del 1919 e che l'obiettivo climatico sia abbinato al bello e all'inclusione sociale.

La verità è che si tratteggia una nuova fisionomia della funzione sociale, ampliativa dei processi di estroflessione dell'ordinamento su istanze personali. Quest'ultima ha infatti progressivamente spostato la sua proiezione da promozione di interessi sociali a quelli ambientali e di educazione/controllo energetico.

Eppure, in sede attuativa, quella medesima funzione, oltre ad esprimersi con ulteriori compressioni del potere dispositivo, si traduce in un aggravamento del costo del bene immobiliare che conduce a un numero crescente di rinunce alla proprietà immobiliare[13].

---

[12] Il riferimento è rinvenibile su Italia Oggi del 15 febbraio 2023, p. 26, f. 1 e su https://www.oice.it/797027/rassegna-stampa-su-comunicato-stampa-su-direttiva-case-green. Per questo, Cortexa (socio fondatore di EAE, l'associazione Europea di Produttori di Sistemi a Cappotto) ha già chiesto al Governo di adottare delle politiche strutturali di incentivazione e di intervenire subito sull'involucro degli edifici affinché non vi siano più sprechi di energia.

[13] La questione ha assunto un rilievo talmente marcato da rischiare di produrre un *vulnus* gestionale nell'area pubblica, per effetto dell'applicazione dell'art. 827 c.c. a un numero cospicuo di immobili vacanti. La questione ha di recente investito – con rinvio pregiudiziale del Trib. L'Aquila – la Corte di Cassazione, la quale è chiamata a interpretare, tra gli altri aspetti, la generalizzata operatività dell'art. 827 c.c., soprattutto con riferimento all'effetto di spettanza del patrimonio immobiliare vacante allo Stato. In merito v. Trib. L'Aquila, Ord., 15 gennaio 2024, n. 2098 e Cass. Ord., 28 febbraio 2024, depositata il 29 febbraio 2024. La documentazione è presente in appendice del volume M. FRANCESCA e L. FOLLIERI (a cura di), *Rinuncia alla proprietà immobiliare*, cit., unitamente allo Studio n. 216-2014/C del Consiglio Nazionale del Notariato, *La rinunzia alla proprietà e ai diritti reali di godimento*, di M. BELLINVIA e al Parere (di massima) dell'Avvocatura Generale dello Stato del 14 marzo 2018, *Rinuncia al diritto di proprietà immobiliare. L'eventuale esperimento dell'*actio nullitatis, di G. PALATIELLO, (già in *Rass. avv. Stato*, 2019, 3, pp. 217 ss.).

Tra le preoccupazioni più chiare della Direttiva sulle case *Green* ve ne sono almeno due che meritano di essere segnalate:

- la prima è rinvenibile nella necessità di evocare un movimento artistico spontaneo di avanguardismo architettonico per giustificare interventi massicci sull'area immobiliare europea;

- la seconda si legge nella spinta inclusiva allorché la Direttiva soggiunge che «Gli edifici inefficienti sono spesso legati alla povertà energetica e a problemi sociali. Le famiglie vulnerabili sono particolarmente esposte all'aumento dei prezzi dell'energia, in quanto spendono una quota maggiore del loro bilancio in prodotti energetici». In questa prospettiva si introduce un nuovo concetto di povertà, quello energetico, che il processo di ristrutturazioni dovrebbe ridurre o prevenire. Ancora, la medesima Direttiva auspica un processo inclusivo di sostegno destinato alle famiglie più vulnerabili (compresi coloro che vivono in alloggi di edilizia popolare). Nella specie si afferma che: «gli Stati membri dovrebbero adottare misure per prevenire gli sfratti alle ristrutturazioni, come limiti agli aumenti dei canoni di locazione». Si discorre così di misure necessarie a «garantire l'equità della transizione».

Traspare, tra le righe, che uno degli obiettivi primari sia il risparmio energetico, funzionale a fronteggiare i costi di un mercato aperto ai venti della concorrenza.

Insomma: la coperta è corta. Scelte macroeconomiche influenzano l'economia fondamentale, creano nuove povertà e nuove discriminazioni tanto da rendere necessarie azioni di intervento sui modelli di consumo e, in questo caso, sulle ragioni strutturali di quei consumi. Resta evidente un dato: l'azione pubblica tira i remi in barca per aprire a un nuovo intervento privato stimolato dall'interesse generale climatico/ambientale e dal miraggio di una ricaduta apprezzabile in punto di costi per il singolo.

È ancora una volta evidente che l'intero obiettivo di sostenibilità (*rectius*: neutralità) climatica passerà necessariamente attraverso un sistema di incentivi che – attesa la forte riduzione del valore risparmio per le famiglie italiane – avvierà un nuovo processo di indebitamento.

Il tutto si colloca infatti su un substrato già fortemente indebolito dalla lunga stagnazione economica che ha colpito, tra gli altri, il settore immobiliare. È la storia dei *subprime rate* che ha fortemente influenzato la domanda di immobili. A ridosso del riferito periodo di stagnazione economica i dati offerti dal Bollettino della Banca d'Italia pubblicato il 13 dicembre 2012 fornivano una fotografia a tratti *noir* dello stato della ricchezza delle famiglie italiane. Essa presentava uno stato della distribuzione concentrato in pochi nuclei familiari, mentre il resto delle famiglie italiane godeva di un livello modesto o nullo di ricchezza; nella specie si affermava che «La ricchezza in abitazioni, a prezzi correnti, è diminuita tra la fine del 2011 e la fine del 2012 del 3,9 per cento (194 miliardi di euro), pari al 6 per cento in termini reali. La crescita media annua, pari al 6,6 per cento nel periodo 1995-2007, si è ridimensionata tra il 2007 e il 2011»[14].

[14] V. *Supplementi al Bollettino Statistico Indicatori monetari e finanziari. La ricchezza delle famiglie italiane*. Nuova serie Anno XXIII – 12 dicembre 2013, p. 8. Sul punto anche U. MATTEI, *Introduzione*, in ID. (a cura di), *Il risparmio immobiliare privato. Bene comune certezza*, Roma, 2013, pp. 9 ss. (spec. p. 10); M. FRANCESCA, *Consumerismo ed effetti della neolingua nel settore immobiliare*, in *Pers. merc.*, 2022, pp. 20 ss.

La situazione attuale non è molto cambiata, anzi – con buona probabilità – è peggiorata in ragione degli scoppi dei conflitti e della fase di inflazione: le famiglie italiane continuano ad avere un evidente problema di risparmio e l'acquisto o la gestione di un immobile ad uso abitativo costituisce mediamente un impegno gravoso. In questo contesto, la gestione di un secondo immobile, magari acquisito per via ereditaria, può rappresentare una scelta impegnativa sia per gli effetti dell'inflazione sul costo delle materie prime e del lavoro (sul piano gestorio) sia e soprattutto per effetto della pressione fiscale.

I dati del sovraindebitamento sono impressionanti, già nel 2019 è stato avvertito[15] che esso «è una piaga sociale che negli ultimi anni ha assunto dimensioni catastrofiche. Basti pensare che, già qualche anno fa, Carlo Milani metteva in evidenza un dato preoccupante: i nuclei familiari sovraindebitati erano passati dai circa 200.000 del 2000 ai circa 1.200.000 del 2012. Una crescita esponenziale del fenomeno, che ha registrato una forte impennata durante la crisi iniziata nel 2008, ma che ha di certo origini più profonde dell'esplodere di quella crisi finanziaria che, dall'America, si è riversata su molta parte del mondo».

La verità con la quale non facciamo i conti è che l'intero sistema finanziario è profondamente cambiato da quella data e che è sempre più marcata la divaricazione sociale tra i redditi[16]. Questo sovraindebitamento è assai lontano dal credito dell'obbligazione borghese, lì dove la funzione – ancora lontana dalla produzione di consumo[17] – era quella di accorciare la distanza tra classi sociali; esso, al contrario, aumenta il divario tra classi sociali con una capacità di cristallizzare le differenze reddituali[18].

Il nostro omino sulla scala di Escher deve riposizionarsi perché il suo futuro, finora garantito dalla certezza della ricchezza immobiliare, non è più roseo. L'incertezza si riverbera anche sulla credibilità finanziaria necessaria per avere accesso a un credito utile a realizzare la ristrutturazione dei suoi immobili.

3. Settore finanziario e sostenibilità.

Un altro omino percorre un'altra scala, quella degli investimenti in titoli finanziari. Il suo contributo alla sostenibilità, in questo caso, si compie

---

[15] M. Musella, *Il sovraindebitamento, alcune riflessioni su cause, effetti e possibili rimedi*, in *Questione Giustizia*, 2019, pp. 284 ss.; in senso più ampio si rinvia a J. Dagnes e M. Filandri, *La finanziarizzazione delle famiglie italiane: trappola o trampolino? Modelli di welfare e modelli di capitalismo. Le sfide per lo sviluppo socio-economico in Italia e in Europa*, Macerata, 2016, pp. 133 ss.; ampie considerazioni in M. Francesca e C. Mignone (a cura di), *Finanza di impatto sociale. Strumenti, interessi, scenari attuativi*, Napoli, 2020.

[16] Sul punto C. Mignone, *Diritti e sostenibilità. Una ricostruzione per immagini*, in *Actual. jur. iberoam.*, 2021, pp. 218 ss., spec. p. 220: «la finanziarizzazione dei servizi essenziali altera la struttura delle disuguaglianze: crea nuove periferie, modifica il paesaggio urbano, espelle coloro che un tempo erano inclusi, pone a rischio di estinzione le comunità più piccole e fragili».

[17] Sia consentito un rinvio a M. Francesca, *Consumerismo ed effetti della neolingua nel settore immobiliare*, cit., pp. 22 ss. e ivi ampia bibliografia.

[18] Sul punto ampiamente R. Cardilli, *Obbligazione e disuguaglianza. Per una lettura critica dell'obbligazione in Friedrich Karl von Savigny*, Bologna, 2021, pp. 87 ss., spec. pp.89 s., dove si discorre «del recupero dell'elemento nascosto di struttura rappresentato dalla guarentigia dell'eguaglianza (…). Lo squilibrio a favore del principio di libertà, slegato da quello dell'eguaglianza, ha spostato l'asse dello schema giuridico a favore dell'indebitamento, come nuova forma giuridica di dipendenza e quindi di controllo delle masse negli ultimi decenni».

attraverso gli ESG. Investimenti di portafoglio con impatti declinati in *Environmental*, *Social and Governance*. La medesima sigla suscita la sensazione di qualcosa di buono. Gli investitori grandi e piccoli (con portafogli medi e piccoli) vengono indagati attraverso la profilatura e vengono introdotti verso politiche di investimento in attività economiche che esprimono sostenibilità nei settori ambientali/sociali, dove la sostenibilità energetica è certamente uno dei pilastri: le parole chiave suonano più o meno così: "investi per il benessere e per il futuro del pianeta"[19].

È difficile immaginare, a questo punto, qualcuno che dia una risposta negativa alla domanda della profilatura che chiede se vi sia interesse a che i prodotti finanziari producano azioni positive, negli evocati settori di benessere collettivo. Come si diceva, essi richiamano impatti di interesse talmente generale da considerarsi in sé una buona cosa da fare. Certo la valutazione tiene prioritariamente conto della propria propensione al rischio, ma è altrettanto noto che il sistema di domande classico di quei piani di sondaggio è modulato su fattori assolutamente eterogenei rispetto alla volontà di salvare il mondo. Quegli indicatori sono infatti tesi a valutare la conoscenza di strumenti finanziari e la relativa propensione al rischio; tuttavia, una risposta avventata può spostare l'acquirente medio di servizi finanziari da un'area moderata a un'area aggressiva, senza rete di salvataggio. Se a ciò si aggiunge la volontà di rischiare per un bene superiore, le porte del mercato del benessere globale si dischiudono. Al fondo è sufficiente avere a disposizione un patrimonio medio-piccolo e una entrata fissa perché il sistema non blocchi l'investitore che decida di percorrere vie più pericolose.

Non si tratterebbe del caso di scuola della insegnante neopensionata che viene erroneamente qualificata come investitore aggressivo e, pertanto, di una situazione in qualche modo giustiziabile, ma di un soggetto che con i suoi piccoli risparmi decide di scegliere la strada degli ESG.

---

[19] In merito R. Lener, *Sostenibilità ESG e attività bancaria*, in *Banca borsa tit. cred.*, 2023, pp. 6 ss.; D. Busch, G. Ferrarini e A. Van den Hurk, *The European Commission's Sustainable Finance Action Plan and Other International Initiatives*, in *EUSFiL Research Working Paper Series*, 2020, 3, disponibile su https://www.eusfil.eu/working-papers. Per effetto di questi interventi, la tutela dell'investitore è stata rafforzata mediante una valutazione del rischio che attualmente impone all'intermediario di incorporare nel flusso informativo – da e verso il cliente – una più ampia gamma di informazioni a carattere "non finanziario", basate sulle preferenze in materia sociale o ambientale del cliente e sulla loro incidenza in termini di rischio/ redditività del prodotto acquistato. Per una compiuta disamina circa il ruolo che l'elemento rischio riveste negli investimenti ESG, si veda M.E. Salerno, *L'integrazione dei fattori di sostenibilità nelle regole di comportamento dell'intermediario finanziario: un ritorno al modello di distribuzione "orientato al prodotto"*, in *Dir. banc. merc. fin.*, 2022, pp. 85 ss.; A. Perrone e A. Cardani, *Servizi di investimento e finanza sostenibile. Le conseguenze non volute della recente disciplina europea*, in *Osservatorio Monetario*, 2022, pp. 86; M. Arrigoni, *Finanza sostenibile, servizi di investimento e tutela dell'investitore*, in *Riv. dir. banc.*, 2023, pp. 261 ss.; F.E. Mezzanotte, *Recent Law Reforms in EU Sustainable Finance: Regulating Sustainability Risk and Sustainable Investments*, in *American University Business Law Review*, 2023, p. 272, secondo il quale la necessaria inclusione nel questionario-MiFID di quesiti relativi alle preferenze di sostenibilità dei clienti non è affatto priva di effetti, ma «comporta una maggior consapevolezza e aumenta la scelta di prodotti coerenti con le preferenze del cliente». In prospettiva critica, analizza invece i limiti che affliggono i meccanismi di *disclosure* e *risk assessment* nel mercato degli investimenti sostenibili: 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. dir. banc.*, 2022, pp. 513 ss.; il problematico bilanciamento tra valutazione del rischio finanziario, redditività dello strumento e obiettivi di sostenibilità sociale è approfondito da C. Mignone, *Investimento a impatto sociale: etica, tecnica e rischio finanziario*, in *Rass. dir. civ.*, 2016, pp. 924 ss.; nonché, più di recente, Id., *La finanza sociale tra tecnica ed ermeneutica*, in *Teoria e prassi del diritto*, 2024, pp. 179 ss.

Ciò premesso, uno dei titoli "buoni" è stato certamente il BNP Paribas *Energy Transition*[20]. Quest'ultimo è un fondo di investimento su energia rinnovabile, ancora attivo, che ha avuto un inizio con guadagni ingenti a tre cifre, ma che dallo scoppio della guerra in Ucraina ha subito una perdita oltre il 70%. La banca ha consigliato ai clienti di trattenere i fondi in portafoglio nella speranza che la bolla speculativa rientrasse; tuttavia, l'effetto panico è proseguito inesorabile fino al momento nel quale i vari consulenti hanno consigliato il disinvestimento. La scelta è stata suggerita a molti clienti per precauzione ma con un ordine ben collaudato nel sistema bancario. Quest'ultimo è generalmente graduato in ragione dell'entità dell'esposizione: prima gli investitori che ne presentano una maggiore e poi via via i più piccoli. L'epilogo è facilmente immaginabile. Gli investitori più piccoli, che hanno deciso di seguire il consiglio e non perdere anche l'ultima parte dell'investimento, hanno perso oltre il 70%; la perdita è aumentata nell'attesa. Certo l'esposizione in quello specifico titolo rappresentava soltanto una parte del portafoglio complessivo di clienti che avevano ricevuto una profilatura con preventiva valutazione della quota di rischio per l'accesso a forme di investimento più o meno rischiose; dunque, si può affermare che il processo di acquisizione di quei titoli non rientri formalmente tra le varie ipotesi collocabili nelle linee degli abusi di mercato[21]. Nella sostanza il comportamento di monitoraggio e i tempi del consiglio di *exit* seguito dalla banca sono certamente espressivi di una prassi squilibrata ma comunque non giustiziabile, in quanto coperta dal consenso informato, che assiste la tutela degli utenti di strumenti finanziari, e dai numerosi fogli dedicati ad avvertire preventivamente il cliente finale circa il rischio dello specifico investimento. Il non detto è che il buono della finalità non impedisce enormi tonfi di quei titoli.

La medesima sorte ha segnato i sottoscrittori dell'ETF *iShares Global Clean Energy*: per questi ultimi investire "pulito" è costato soltanto il 23% (nel 2023)[22] in meno dell'investimento iniziale.

Tutt'altro scenario dall'altra parte del mondo, nella metà oscura. Le ETF *World Energy* hanno guadagnato il 197% nell'ultimo triennio[23] nel settore dell'energia non sostenibile.

La spiegazione è presto data: le aziende che realizzano progetti eolici e solari dipendono fortemente dal mercato del debito[24]. Quando quel mercato è costoso, l'operazione economica complessiva ne risente in termini di capacità di produrre utili per gli investitori. Dal canto delle energie fossili, queste hanno beneficiato dell'aumento dei prezzi legato alla guerra in Medioriente.

---

[20] Un grafico efficace si trova su https://www.morningstar.it/it/funds/snapshot/snapshot.aspx?id=F00000PXGZ dove è significativamente specificato che a partire dal 1° settembre 2019 «La strategia di investimento del fondo è cambiata in misura significativa rispetto alla precedente al punto tale da non ritenere opportuno considerare metodologicamente valide le performance storiche antecedenti a tale data, che non vengono quindi visualizzate».

[21] Sul concetto di abuso commerciale cfr. M. ORLANDI, *Dominanza relativa e illecito commerciale*, in G. GITTI e G. VILLA (a cura di), *Il terzo contratto*, cit., pp. 137 ss., spec. p. 163 ss.

[22] Cfr. il grafico https://www.morningstar.it/it/etf/snapshot/snapshot.aspx?id=0P0000M64O.

[23] I dati sono rinvenibili su https://www.morningstar.it/it/etf/snapshot/snapshot.aspx?id=0P00017PP3.

[24] È noto che le bolle speculative più rischiose siano quelle prodotte/finanziate dal credito bancario, sul punto v. G. VACIAGO, *La prima crisi finanziaria globale*, in *Riv. trim. di cultura e di politica*, 2008, pp. 1047 ss.

Il non detto ai risparmiatori – che decidano di investire parte del loro risparmio in attività sostenibili – è che investire "buono" reca in sé un profilo di rischio molto più alto di quello puro d'impresa. Si tratta del rischio dell'innovazione che da sempre sconta un'alea maggiorata. La letteratura economica e finanziaria ne narra le vicende a partire dal '600, dal mercato dei tulipani e dall'effetto bolla nella storia degli investimenti in realtà innovative[25], tra cui la nota questione del crac della borsa di Vienna del 1873 e della connessa *débâcle* prodotta dalla febbre ferroviaria in Svizzera[26].

L'assenza di un simile dato non è allora una carenza informativa del procedimento formativo a tutela dei c.dd. contraenti deboli. Non è un abuso di mercato, è un dato che gli investitori professionali ben conoscono, ma di certo non rientra nel dato esperienziale o di conoscenza che può essere contenuto in plichi di fogli illustrativi dell'investimento. A ciò si aggiunge il *battage* a proposito della sostenibilità a tutti i costi e dell'impegno sociale e ambientale cui tutti siamo esortati a rispondere.

Il settore di mercato coperto dalla bandiera della sostenibilità vanta qualcosa in più del mero mercato innovativo dei tulipani o dei *computer* degli anni '80, è un mercato finanziario colorato da elementi politici, economici e ambientali di rilievo globale-esistenziale. Si tratta, in fin dei conti, di una marcia in più sul piano dell'attrazione: è la sensazione di aver partecipato a qualcosa di buono che da un lato incoraggia e dall'altro fa perdere la minima resistenza critica. È la forza di un nuovo «marchio»[27] economico-politico: la sostenibilità[28].

---

[25] V., in particolare, L. BAZZICALUPO, *Comportamenti di massa e automatismo nei mercati finanziari*, in *Filosofia politica*, 2021, pp. 103 ss., spec. p. 114, la quale pone in rilievo come le bolle speculative siano eventi costanti dei mercati finanziari: «La conclusione del nostro percorso ci presenta la scena di un dramma che mette in discussione radicalmente il presunto equilibrio auto-efficiente dei mercati finanziari e la autonomia onnisciente dell'attore economico. È un dramma che si ripete: dal tracollo della borsa dei tulipani del 1637 (l'assurda casualità e irrilevanza del contenuto della convenzione!) al *Mississippi (Law) Schema* in Francia e la *South Sea bubble* britannica del 1720, al crollo delle borse di Parigi e Lione nell'1882, al canonico venerdì nero di Wall Street con la conseguente tragica depressione; fino al susseguirsi incalzante di crisi dopo la deregulation finanziaria: il 1987 prima crisi *infotech*, il 1997-8 la crisi asiatica, il 2000 la bolla di Internet, il 2002 il crollo di Enron e Worldcom, il 2008 i subprime, il 2011 i debiti sovrani...». Discorre di autoreferenzialità della finanza e di rischio finanziario endogeno al medesimo sistema S. ZAMAGNI, *La lezione e il monito di una crisi annunciata*, in *Sistemi intelligenti*, 2009, pp. 293 ss.

[26] V. P. FEMIA, *Sentimento e moltitudine. Rudolf von Jhering tra interessi ideali e beni comuni*, Bologna, 2024, pp. 41 ss., il quale richiama le posizioni di Jhering e Meli sulla nota vicenda del crac della borsa di Vienna del 1873 e sugli effetti sull'affare delle ferrovie svizzere. Qui si legge, muovendo dal parere di Jhering, che «La crisi incombente, determinata anche da lavori intrapresi al solo fine di approfittare per speculazioni finanziarie, ebbe in Svizzera l'effetto di concentrare i lavori sulla costruzione di reti secondarie […]. Qui interviene un elemento economicamente cruciale, che dal parere resta in ombra, ma è il motore di tutte le controversie: il 1873 è l'anno della Grande depressione, la prima grave crisi del capitalismo moderno».

[27] In realtà, concetti quali competitività, coesione sociale e, appunto, sostenibilità non sono altro che "marchi della conoscenza" (*knowledge brand*), nel senso chiarito da N.-L. SUM, *The production of hegemonic policy discourses: 'competitiveness' as a knowledge brand and its (re)contextualizations*, in *Crit. pol. studies*, 2009, pp. 184 ss., 191: «[l]ike commercial brands, knowledge brands address the rational and irrational aspects of human nature. Emotionally, it addresses pride, anxieties, threats, and social tensions linked to growth or decline, development, and the intense pressures of economic restructuring in globalized information age. These rational and irrational effects shape struggle to make a brand hegemonic».

[28] Secondo C. MIGNONE, *La sostenibilità in altre parole. Divagazioni di un civilista a partire da un esperimento mentale*, in *Il foro napoletano*, 2023, 4, pp. 644 s., sarebbe utile simulare la «scatola nera» del concetto: [c]omprendere chi introduce parole come questa nel discorso, chi le elabora, in base a quali analisi e riflessioni; quali interessi ne escono rafforzati, quali indeboliti. Rispondere a queste domande è fondamentale […] per chi il diritto è chiamato ad applicarlo e, in vista della sua applicazione, a interpretarlo. Insomma, per tutti coloro che vogliono parlare di sostenibilità anziché *essere parlati*».

Nelle riferite situazioni economiche di bolla del mercato innovativo, gli investitori professionisti o con ingenti capitali hanno con buona probabilità coperto il rischio connesso all'investimento innovativo e hanno informazioni sufficienti a gestire l'uscita. Insomma: amministrano il proprio investimento privi di emozionalità e/o empatia. Il risparmiatore medio che ha deciso di supportare le politiche ESG, perché partecipe della politica ambientale e/o della necessità di intervenire su una qualsiasi politica sociale, tratta il proprio investimento con un approccio emotivo, privo degli anticorpi necessari per affrontare dinamiche di mercato anche più pericolose di quelle dei mercati tradizionali.

E allora non è esclusivamente una prospettiva rimediale relativa al micro-rapporto che può conferire sicurezza a un mercato finanziario puro, quale quello degli ESG, ammantato da politiche salvavita e di interesse generale. Quelle nulla possono circa la pericolosità insita di un settore fortemente innovativo e, dunque, instabile, nel quale salta l'equilibrio anche della speculazione: «tra guadagno e perdite»[29]. Come si è avuto modo di riferire, non si tratta di una instabilità propria di ogni settore innovativo; ad essa si aggiunge la proiezione ideologica e/o politica che annacqua proprio quella razionalità ricercata e indotta dai moduli di valutazione del cliente e dalle procedimentalizzazioni del consenso.

Dunque, l'apertura a soggetti non professionali per l'accesso ai c.dd. capitali pazienti per il perseguimento di politiche sociali o ambientali necessita di altrettanti strumenti di sostegno, idonei a presidiare l'investimento o comunque i suoi costi. L'apertura oltre il mercato professionale dovrebbe essere accompagnata quanto meno dalla riduzione dei costi della tassazione o dei costi di gestione o dall'obbligo di inserire clausole di salvaguardia per quegli investitori non qualificabili come professionali.

Anche questa scala apre scenari pericolosi per il secondo anonimo protagonista, che per questa via rischia il proprio risparmio, spesso necessario per affrontare periodi complessi della vita di ciascuno: una perdita nel settore finanziario potrebbe incidere sull'economia fondamentale del singolo e aprire ad esigenze futuribili di sostegno.

4. Settore energetico e sostenibilità.

Il terzo settore è quello del mercato energetico *retail*. Tra gli scenari che incidono sul reddito disponibile vi è sicuramente il fattore costo dei servizi insopprimibili. Ritorna il mercato energetico e questa volta l'obiettivo della sostenibilità è raggiunto anche attraverso il mercato concorrenziale: l'utente

[29] Giocano bene le parole di R. VON JHERING, *Lo scopo del diritto*, trad a cura di M.G. LOSANO, Torino, 2014, p. 173 e ripreso da P. FEMIA, *o.u.c.,* p. 45: «Se gli effetti disastrosi delle società per azioni si fossero limitati alle persone direttamente interessate si potrebbe sempre dire che avrebbero dovuto stare più attente, anche se la stupidità non autorizza l'inganno nell'imprudenza il furto. Ma nel danno è stata coinvolta tutta la società. Le società per azioni sono riuscite a scuotere, in ogni settore e nel modo più catastrofico, l'equilibrio economico su cui riposa l'intero nostro ordinamento e la sicurezza nel sistema dei traffici: nell'acquistare e nell'affittare hanno scosso l'equilibrio tra il prezzo e la merce; nello speculare, quello tra guadagno e perdita; nel produrre, quello tra bisogno e produzione».

energetico è finalmente in condizione di scegliere il contratto di fornitura più efficiente.

Anche in questo caso c'è un non detto e riguarda gli effetti della trasformazione di mercato: un bene essenziale è oggetto di promozioni aggressive che superano gli albori della contrattazione fuori dai locali commerciali, quando gruppi di anziani venivano condotti in gita per indurli all'acquisto di improbabili *set* di pentole[30].

Tra le diverse modalità di promozione commerciale, il c.d. *teleselling* è certamente quella più ricorrente e minacciosa. La questione ha acquisito immediata centralità: le autorità indipendenti ne hanno dichiarato la pericolosità (ACGM, 2 novembre 2022, n. 30373), per poi avviare una campagna di comunicazione, "DIFENDITICOSì", per fornire ai consumatori consigli e informazioni per proteggersi dall'insistenza o dalla scorrettezza di alcuni *call center* (AGCM e ARERA, Comunicato 24 giugno 2022). È noto il procedimento nato a seguito delle numerose segnalazioni di consumatori e associazioni che hanno evidenziato l'ingannevolezza di un messaggio preregistrato diffuso da un'operatrice di segreteria telefonica di Enel e da operatori di *call center*, riguardante la data di cessazione del regime di maggior tutela per i clienti finali di piccole dimensioni (mercato tutelato), indicato come imminente e, contrariamente al vero, come obbligatorio. All'ingannevolezza dell'informazione, l'autorità garante della concorrenza e del mercato – nel provvedimento AGCM, n. 30373/2022 – ha affiancato la condanna per pratiche commerciali aggressive, a causa delle insistenti e ripetute telefonate che diffondevano il messaggio preregistrato, anche dirette ai moltissimi consumatori che non avevano fornito un preventivo consenso ad essere contattati per finalità di *marketing*.

A poco sono serviti i richiamati provvedimenti. Proprio di recente il Garante per la protezione dei dati personali ha sanzionato ENI Plenitude[31] per alcune pratiche di *telemarketing*. Il Garante ha contestato a ENI chiamate promozionali effettuate senza il consenso dell'interessato o rivolte a numeri iscritti al Registro pubblico delle opposizioni[32]. A ciò si aggiunge il numero enorme di contratti acquisiti attraverso le riferite attività illecite.

Il Garante ha fondato il provvedimento su 108 segnalazioni e 7 reclami pervenuti all'Autorità nel periodo compreso fra settembre 2021 e marzo 2023 tutte relative al *telemarketing*.

È una nuova deriva della promozione commerciale[33], che tuttavia incide su un bene essenziale tanto da rendere sostanzialmente ininfluente, nella

[30] Sia consentito rinviare a M. FRANCESCA, *Bene-energia. Abusi di mercato e nuovi domini*, in *Nuovo diritto civile*, 2023, pp. 21 ss.

[31] Cfr. provvedimento AGCM n. 342 del 6 giugno 2024.

[32] È interessante notare quanto emerso in uno studio su campioni del 2017, qui si osserva «come anche coloro che dichiarano di aver interesse per la protezione dei propri dati personali (supra n. 1), di regola non prestano attenzione o, in ogni caso prescindono dall'informativa sulla privacy, anche in un ambiente non naturale (l'esperimento) ove i soggetti sono espressamente richiesti di eseguire il compito. Le decisioni in materia di consenso al trattamento dei dati personali prescindono totalmente dai giudizi più generali sulle attività cui il trattamento dei dati è funzionale e sulle scelte in proposito, nonché sul tenore stesso dell'informativa»: L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2017, pp. 363 ss.

[33] Cfr. provvedimenti AGCM n. 19846 del 7 maggio 2009; n. 21916 del 15 dicembre 2010; n. 23011 del 23 novembre 2011. Tutti i citati provvedimenti riguardano pratiche scorrette poste in essere da agenti

dinamica riparatoria, l'esercizio del diritto di recesso, quale presidio a tutela dell'utente nelle contrattazioni a distanza o, comunque, fuori dai locali commerciali.

Infatti, nel micro-rapporto, il singolo utente avrà contezza, sulla propria economia, degli effetti di quei contratti conclusi soltanto con il pagamento della prima fornitura[34]. A questo punto, egli potrà esercitare il diritto di recesso con *switching* ad altro operatore, ma il danno sarà ormai manifesto in tutta la sua portata[35].

Certo egli ha dalla sua parte la possibilità di avviare una procedura di reclamo nei confronti del proprio operatore e nei confronti di ARERA per denunciare l'illiceità delle procedure, per ricevere – quando tutto va bene – delle scuse o dei *bonus* su servizi esterni.

Nel mentre egli subisce uno *stress*, legato alla ricerca di un terzo fornitore, con un piano modificato dei costi di mercato e non necessariamente pari a quanto previsto all'interno del primo contratto.

Non si tratta insomma di rinunciare ad un paio di scarpe che non piacciono o calzano strette e tantomeno di rispedire un bene che non corrisponde alle qualità pubblicizzate, l'energia è un servizio irrinunciabile e un errore di valutazione determina uno stato di incertezza per il futuro circa l'entità di costi insopprimibili[36].

---

commerciali. Una diffusa analisi in F. POLETTINI, *o.u.c.* In merito v. anche AGCM, Relazione annuale sull'attività svolta - 2013, Principali interventi nei diversi settori economici, pp. 178 ss. V., ancóra, AGCM 4 novembre 2015, Enel Energia S.p.a., Enel Spa *vs.* Federconsumatori, Codacons, Tutela Noi Consumatori, Movimento Difesa del Cittadino e Codici Onlus - Centro per i Diritti del Cittadino, ancóra in materia di «forniture non richieste» e dove l'Autorità torna sul comportamento degli agenti sui mercati energetici e del gas «Su entrambi i mercati della vendita sul mercato libero di energia elettrica e di gas naturale, la conclusione dei nuovi contratti di fornitura viene principalmente realizzata da EE sulla base di appositi contratti di appalto di servizi e/o di agenzia, utilizzando imprese terze che contattano con proprio personale i possibili clienti per via telefonica (c.d. "*teleselling*") o attraverso incaricati che si recano di persona presso i possibili clienti (c.d. vendite "*porta-a-porta*"), oltre che attraverso i c.d. "Punti Enel Negozi *Partner*" ("PENP"), punti fisici di vendita gestiti da terzi».

[34] Sui meccanismi persuasivi e sui rischi del «pantano informativo» nel mercato energetico v. l'interessante analisi di M. NIGRO, *Informazione contrattuale e mercato energetico: dalla 'spinta gentile' alla manipolazione cognitiva*, in *Rass. dir. civ.*, 2024, in corso di pubblicazione.

[35] Sulle peculiarità del rimedio del diritto di recesso nel particolare contesto di fornitura energetica v. A. SARDINI, *Regolazione di settore e diritto di recesso*, cit., pp. 242 ss., il quale osserva che «a seguito della delibera 302/2016/R dell'allora Autorità per l'energia elettrica e il gas, così come modificata dalla successiva delibera 783/2017/R/com, i clienti finali di piccole dimensioni – siano o non siano serviti in regime di tutela – lo esercitano secondo tempistiche e modalità predeterminate dall'*authority* stessa, le quali variano non poco a seconda che il rimedio venga o meno esercitato in funzione del successivo *switching*. Nel caso in cui la volontà di sottrarsi al vincolo negoziale venga manifestata per finalità che esulano dall'intenzione di cambiare il venditore, il termine entro il quale dovrà avvenire la comunicazione dovrà essere di almeno un mese; le modalità di esercizio, poi, non si discosteranno concretamente dalla disciplina di parte generale, in quanto il recesso sarà «esercitato direttamente dal cliente finale nei confronti del venditore uscente». Diversamente, laddove il cliente intenda eseguire il passaggio dal precedente venditore ad un altro, i tempi e le modalità di esercizio del rimedio risulteranno differenti rispetto a quanto previsto in via generale. I primi subiranno una lieve contrazione, attestandosi ad almeno tre settimane, stante la previsione per la quale la manifestazione della volontà di svincolarsi unilateralmente dal rapporto dovrà essere comunicata al venditore uscente entro il giorno 10 del mese antecedente la data del passaggio. Con riferimento, invece, al *quomodo*, l'autorità ha previsto una disciplina che – avendo riguardo a profili specifici – si discosta fortemente dalle previsioni codicistiche e consumeristiche. In particolare, il comma 3.1 dell'Allegato A1 alla delibera n. 783/2017/R/com dispone che, nel caso in esame, il cliente finale debba rilasciare al venditore entrante apposita procura a recedere, in nome e per conto proprio, dal contratto in essere con il venditore uscente».

[36] Sul punto già P. PERLINGIERI, *La tutela del consumatore tra liberismo e solidarismo*, in ID., *Il diritto dei contratti tra persona e mercato. Problemi del diritto civile*, Napoli, 2003, p. 99. V. anche le considerazioni di G. CARAPEZZA

La reazione ordinamentale è stata ulteriore e si rintraccia nel sistema di conciliazione obbligatoria, funzionale a garantire una giustizia *portable* al nuovo consumatore di beni energetici. A partire dal 1° gennaio 2017 è entrato in vigore il testo integrato in materia di procedura di risoluzione stragiudiziale delle controversie tra clienti finali ed operatori o gestori nei settori regolati dall'Autorità per l'energia elettrica, il gas e il sistema idrico[37]. Con il riferito provvedimento è stabilita l'obbligatorietà del tentativo di conciliazione per la risoluzione delle controversie già segnalate con reclamo e non risolte con l'operatore. L'esperimento del tentativo di conciliazione è condizione di procedibilità della domanda giudiziale a norma dell'art. 2, comma 24, lett. *b*, l. 14 novembre 1995, n. 481 e dell'art. 141, comma 6, lett. *c*, c. cons.

La scelta di sistema è peculiare, si opera attraverso le ADR cui è attribuito l'effetto di esecutività del titolo conciliativo, in genere proprio delle procedure di conciliazione giudiziaria. Qui invece opera un congegno ibrido: l'obbligatorietà delle medesime è abbinata a un procedimento innanzi all'ARERA. In genere le ADR (o ODR) sono facoltative o al più obbligatorie per la sola parte professionista[38]: non sono mai sostitutive o di impulso all'apertura di un contenzioso canonico.

L'effetto voluto è palese ed è lontano dalla ricerca del torto e della ragione: controllare lo stato di litigiosità prevedibile in un mercato portatore di un bene primario e per il quale è necessario trasmettere fiducia al consumatore circa la

---

FIGLIA, *I rapporti di utenza dei servizi pubblici tra autonomia negoziale e sussidiarietà orizzontale*, in *Rass. dir. civ.*, 2017, pp. 440 ss., il quale osserva: «Territori un tempo presidiati da discipline e categorie di matrice pubblicistica sono stati attratti alla dimensione paritetica dello *ius civile* a tal punto da coniarsi nuovi paradigmi, come quello dei "contratti di utenza pubblica": un concetto che costituisce espressione riassuntiva dei rapporti ove l'erogazione alla massa dei consumatori – in regime di monopolio o di concorrenza, da parte di un soggetto pubblico o privato – ha ad oggetto beni o servizi "essenziali per la vita umana"».

[37] Delibera ARERA del 5 maggio 2016, n. 209.

[38] Il regolamento 524/2013/UE del Parlamento europeo e del Consiglio del 21 maggio 2013 (regolamento sull'ODR per i consumatori) richiama infatti la procedura già prevista per le ADR dalla direttiva 2013/11/UE del Parlamento europeo e del Consiglio del 21 maggio 2013. In entrambi i provvedimenti è presente il richiamo alla Libertà (art. 10 della direttiva 2013/11/UE). In particolare, si stabilisce che: «1. Gli Stati membri provvedono affinché un accordo tra un consumatore e un professionista riguardo alla presentazione di reclami presso un organismo ADR non sia vincolante per il consumatore se è stato concluso prima dell'insorgere della controversia e se ha l'effetto di privare il consumatore del suo diritto di adire un organo giurisdizionale per la risoluzione della controversia. 2. Gli Stati membri provvedono affinché nelle procedure ADR volte a comporre la controversia mediante l'imposizione di una soluzione, sia possibile rendere tale soluzione vincolante per le parti soltanto a condizione che queste siano state preventivamente informate del suo carattere vincolante e abbiano specificatamente dato il loro assenso. La specifica accettazione del professionista non è richiesta se le norme nazionali dispongono che le soluzioni vincolano i professionisti».
Più ampiamente, tra la numerosa letteratura in argomento, v. le riflessioni di E. CAPOBIANCO, *Dai sistemi di risoluzione alternativa delle controversie nell'ordinamento italo-comunitario alla mediazione*, in *Vita not.*, 2012, pp. 155 ss.
Che vi sia un problema di effettività di tutela dei consumatori è evidente anche dall'intervento della Direttiva 2020/1828/UE, alla base dell'introduzione dell'art. 140-*ter* ss. c. cons., al quale dedica una incisiva analisi E. CAMILLERI, *L'azione rappresentativa e il raccordo imperfetto con il diritto privato regolatorio. Le decisioni delle authorities tra libero apprezzamento e presunzioni giurisprudenziali: spunti dall'*arrêt repsol, in NLCC, 2024, pp. 437 ss. Qui si osserva che «non mancano elementi, a partire dall'opzione terminologica di fondo (azione "rappresentativa", in luogo di azione "di classe"), che inducono a scorgere quasi una sporgenza della tecnica sulla tutela e così, in fin dei conti, una recessività dell'*access to justice* propriamente inteso – ossia di tipo individuale, quando pure in forma aggregata – rispetto a esigenze di "governo equilibrato" e di "uso razionale" della risorsa scarsa-giurisdizione, il ricorso alla quale è qui in effetti propiziato ma "in favore della collettività indistinta"».

tutela dei propri interessi[39]. Il riferito effetto assume poi una contezza ulteriore nei patti di non divulgazione che generalmente accompagnano il processo di conciliazione e i relativi esiti, sì da togliere voce al contenzioso.

Il risultato è stato enorme. La medesima ARERA ne offre un quadro chiaro. Nella relazione annuale[40] la riferita Autorità rileva che si assiste a un «aumento pressoché generalizzato delle richieste scritte volte ad attivare gli strumenti di supporto per la gestione di specifiche problematiche – come le procedure speciali risolutive nei settori energetici (+ 40% rispetto al 2022) – o di risoluzione delle controversie di tipo conciliativo (le domande al Servizio conciliazione sono aumentate di oltre 8.300 unità da un anno all'altro)».

Non vi è dubbio, come già osservato, che il sistema delle *ADR* offra una sensazione di giustizia *portable* senza costi di accesso, ciò nondimeno il medesimo risultato sarebbe stato raggiunto con l'obbligatorietà dell'ADR per la sola parte professionista e attraverso la costituzione per l'utente di vie parallele: ADR e/o giustizia ordinaria. La scelta alternativa avrebbe consentito all'utente l'immediata ricerca della soluzione più idonea a giustiziare il proprio contratto.

Il danno, in molti casi, si manifesta con la perdita di un contratto di fornitura più favorevole rispetto a quanto rinvenibile sul mercato in un tempo successivo, con un pregiudizio destinato a proiettarsi nel tempo sotto forma di un maggior costo complessivo per fruire di un servizio oggettivamente di prima necessità. In un simile stato delle cose gli elementi assorbenti sono due:

a) il risarcimento tabellare fissato dall'ARERA[41], a seconda della violazione subita dall'utente finale, poco si presta a compensare il consumatore di servizi energetici per «forniture non richieste»[42]. Questa è certamente l'ipotesi più

[39] Sia consentito il rinvio a M. FRANCESCA, *Dalle ADR offline alle procedure di Online Dispute Resolution: statuti normativi e suggestioni di sistema*, in *Corti Salernitane*, 2015, pp. 7 ss.; Con riferimento alle ODR v. le considerazioni di A. FACHECHI, *La giustizia alternativa nel commercio elettronico. Profili civilistici delle* ODR, Napoli, 2016, pp. 117 ss., la quale lucidamente conclude che le ODR garantiscono un alto profilo di riservatezza: «Avere l'opportunità di rimuovere il malcontento dei consumatori con procedure extragiudiziali, specie *online*, e preferibile, poi, per i professionisti (soprattutto per quelli noti nel settore di riferimento) che temono un pregiudizio alla propria reputazione – e, dunque, al proprio potere di mercato – dalla diffusione di informazioni sul contenzioso avviato». Ma prima ancora si rinvia alle avvincenti pagine di L. NADER, *Le forze vive del diritto. Un'introduzione all'antropologia giuridica*, Napoli, 2003, spec. pp. 110 ss.

[40] ARERA, Relazione annuale, Attività svolta 2023, Volume 2.

[41] Si rinvia a mero titolo informativo alla Deliberazione ARERA, 18 novembre 2008, ARG/com 164/08, *Testo integrato della regolazione della qualità dei servizi di vendita di energia elettrica e di gas naturale*. V. anche Allegato A alla deliberazione 463/2016/R/com del 4 agosto 2016 – versione modificata e integrata dalle deliberazioni 738/2016/R/com del 6 dicembre 2016, 555/2017/R/com del 27 luglio 2017, 242/2021/R/com dell'8 giugno 2021 e 269/2022/R/gas del 21 giugno 2022, *Testo integrato delle disposizioni dell'autorità per l'energia elettrica il gas e il sistema idrico in materia fatturazione del servizio di vendita al dettaglio per i clienti di energia elettrica e di gas naturale*.

[42] È proprio l'ARERA a soffermarsi sul punto nel DCO n. 46/11, "*Documento per la consultazione emanato nell'àmbito del procedimento avviato con deliberazione 15 dicembre 2011, ARG/com 185/11. Mercati di incidenza: energia elettrica e gas naturale*" cit., pp. 4 ss., l'ARERA ha avuto modo di osservare che «Le principali criticità connesse all'attivazione di contratti non richiesti, invece, sono risultate attinenti, da un lato, al danno economico (oneri da sopportare per il ritorno con il precedente fornitore, costi connessi ad eventuali tardivi conguagli ed eventuali richieste di pagamento da parte delle agenzie di recupero crediti) ed esistenziale patito dal cliente finale, dall'altro, all'omesso o carente controllo degli operatori sull'attività posta in essere dalle agenzie di commercializzazione, con rinvio a queste della responsabilità da parte degli operatori in caso di segnalazioni di pratiche commerciali scorrette». Ampiamente sul punto F. POLETTINI, *Attivazioni contrattuali non richieste di utenza gas ed energia elettrica e pratiche commerciali scorrette*, in *Dir. ind.*, 2012, pp. 460 ss.

ricorrente nella quale confluiscono patologie diverse[43] (carenza di consenso, carenza di sottoscrizione del contratto, informazioni ingannevoli, contratti intervenuti su *telemarketing* illecito) che conducono all'inidoneità a produrre un'obbligazione a titolo di corrispettivo per l'intervenuta fornitura di beni o servizi non voluti. Il riferimento è all'art. 66 *quinquies* c. cons.[44] sebbene declinato in modo ampliativo sia dall'ARERA sia dall'AGCM[45].

b) il sistema delle conciliazioni dà vita a una sorta di "giustizia" muta, di natura commutativa e privata dell'effetto conoscenza (pubblicazione). Quest'ultimo è invece notoriamente utile a fungere da monito sul piano di sistema per l'operatore commerciale e a innescare il meccanismo imitativo per altri utenti, come dimostra – sul piano macroeconomico – la sanzione relativa alla pubblicazione degli esiti dell'accertamento da parte delle Autorità garanti.

Quella "giustizia" muta si trasforma in un mero costo di transazione preventivabile e soprattutto bilanciabile con le enormi entrate prodotte da contatti (*telemarketing*) illeciti.

Il terzo omino delle scale di Escher non ha un percorso migliore degli altri. Nel tentativo di riequilibrare la posizione lesa nel mercato di un bene essenziale, egli:

1) deve affrontare il tentativo obbligatorio di conciliazione, con il rischio di trovare la sua posizione tutelata nei limiti di risarcimenti tabellari.

Certo l'accesso alle ADR è gratuito e consente di trovare soluzioni equilibrate senza particolari oneri. Il rischio è tuttavia rintracciabile

---

[43] Ampiamente già G. PERLINGIERI, *Regole e comportamenti nella formazione del contratto. Una rilettura dell'art. 1337 codice civile*, Napoli, 2003, pp. 85 ss., spec. pp. 153 ss.; ID, *L'inesistenza della distinzione tra regole di comportamento e di validità nel diritto italo-europeo*, Napoli, 2013, pp. 9 ss., il quale riconnette la selezione del rimedio all'effettiva incidenza della scorrettezza sul rapporto. Centrale è l'osservazione circa la concreta portata della regola di comportamento sulla libera formazione della volontà: nullità per illegalità, *rectius* mancanza dell'accordo per mancanza totale della volontà. V. anche ID., *La convalida delle nullità di protezione e la sanatoria dei negozi giuridici*, Napoli, 2011, pp. 75 ss.

[44] L'art. 66-*quinquies*, c. cons., attualmente stabilisce che: «Il consumatore è esonerato dall'obbligo di fornire qualsiasi prestazione corrispettiva in caso di fornitura non richiesta di beni, acqua, gas, elettricità, teleriscaldamento o contenuto digitale o di prestazione non richiesta di servizi, vietate dall'art. 20, comma 5, e dall'art. 26, comma 1, lettera f), del presente Codice» (come modificato dal d.lgs. 21 febbraio 2014, n. 21). In tema di «forniture non richieste», v. G. DE CRISTOFARO, *Le ''prestazioni non richieste'' nelle esperienze giuridiche europee fra contratto, illecito e* indebiti solutio, Milano, 2004, *passim*; ID., *Le forniture non richieste*, in ID. (a cura di), *Le ''pratiche commerciali sleali'' tra imprese e consumatori. La direttiva 2005/29/CE e il diritto italiano*, Torino, 2007, pp. 303 ss.; M. FRANZONI (a cura di), *Codice ipertestuale del consumo*, Torino, 2008, pp. 344 ss.; L. TAFARO, *Forniture non richieste: valore negoziale del silenzio e procedimenti formativi del contratto*, in *Notariato*, 2008, pp. 620 ss.; F. POLETTINI, *o.u.c.*; F. LONGOBUCCO, *Forniture non richieste e procedimentalizzazione dell'attività d'impresa: doveri di* status *del professionista?*, in *Giur. it.*, 2014, p. 2623 ss.; V. AURICCHIO, *Fornitura non richiesta*, in A.M. GAMBINO e G. NAVA (a cura di), *I nuovi diritti dei consumatori. Commentario al d.lgs. n. 21/2014*, Torino, 2014, pp. 349 ss.

Sull'evoluzione normativa v. G. DE CRISTOFARO, *Il regime privatistico ''speciale'' delle c.d. forniture non richieste: la prima presa di posizione della Suprema Corte*, in *Nuova giur. civ. comm.*, 2021, p. 575 ss., il quale ritorna sulla questione in occasione della pronuncia Cass., ord., 12 gennaio 2021, n. 261, in *One-legale.it*. Sul punto v. anche F. LONGOBUCCO, *o.u.c.*, p. 2620, secondo il quale «Non mancano invero alcuni profili di novità. Il nuovo art. 66-*quinquies*, c. cons., assume anzitutto portata ampliativa nel sistema. La disciplina sulle «forniture non richieste» viene espressamente estesa al settore (certamente più vulnerabile) dei servizi pubblici essenziali per la persona (acqua, gas, elettricità, teleriscaldamento o contenuto digitale). Ciò coerentemente con il campo applicativo generale del d. lgs. n. 21/2014, alla cui stregua ''rientrano fra i beni oggetto della presente direttiva l'acqua, il gas e l'elettricità, quando sono messi in vendita in un volume delimitato o in quantità determinata''. I prodotti a contenuto digitale (licenze, softwares, ecc.) sono invece richiamati nel considerando n. 19 della Dir. 2011/83/UE». Diffusamente sul punto M. FRANCESCA, *Bene-energia,* cit., pp. 30 ss.

[45] V. M. FRANCESCA, *o.l.u.c.* Nella prospettiva ampliativa anche l'Autorità Garante della Concorrenza e del Mercato; riferisce diffusamente in merito F. LONGOBUCCO, *o.u.c.*, pp. 2623, nota 27.

nell'equilibrio di una giustizia tutto sommato commutativa attraverso la quale le parti riconoscono oneri e benefici reciproci[46], questi ultimi assai lontani dal ricomporre l'equilibrio ormai incrinato[47], ma funzionali comunque a ricomporre il disagio dell'utente senza ulteriori peregrinazioni alla ricerca di soluzioni migliori;

2) nel caso di risultato insoddisfacente della conciliazione, il medesimo utente potrebbe finalmente adire il giudice ordinario. Certo per raggiungere questo risultato, deve superare la condizione di procedibilità che impone il tentativo di conciliazione, non lasciarsi tentare dal canto delle sirene della gratuità di un risultato di compromesso e scegliere di affrontare un aggravio di costi per proseguire nella ricerca di un concreto risarcimento della posizione contrattuale lesa[48]. Nel caso di specie, la vicenda seguirebbe le linee applicative dell'art. 66 *quinquies* c. cons., con potenziale riconoscimento di un risarcimento concretamente riequilibratore della congerie di interessi lesi, comprensiva della parte non patrimoniale.

Così attuato l'obiettivo di sostenibilità si spiega in una pluralità di direzioni[49], sicuramente teso alla futuribilità di scelte attuali ma – nei fatti – produttivo di enormi sperequazioni e potenziale fonte di processi di divaricazione sociale.

---

[46] In questo caso resta la ricerca tra le parti di una giustizia, in fin dei conti, ancóra commutativa e in merito alla quale F. DENOZZA, *Disciplina del contratto e "*non – moral goods*"*, in M. MAUGERI e G. GRASSO (a cura di), *Contratto, Contratti e mercati*, Roma, 2022, pp. 345 ss., spec. pp. 352 ss. richiama mirabilmente la riflessione sui problemi della giustizia distributiva di C. TAYLOR, *The Nature and Scope of Distributive Justice*, in *Philosophical papers*, Vol. 2, *Philosophy and the human sciences*, Cambridge, 1985, pp. 289 ss. e osserva: «La giustizia dipende dal contesto. Ce lo insegna già uno dei testi fondanti della nostra civiltà. È l'inizio folgorate dell'Iliade: Agamennone deve rinunziare alla sua schiava e restituire la fanciulla al padre, per compiacere, nell' interesse dell'intera spedizione, Apollo. Prende allora in cambio la schiava di Achille. C'è giustizia commutativa in questa serie di interazioni?».

[47] Cfr. A. CIATTI, *Poteri di regolazione delle* Autorithies*, sopravvenienze normative e rapporti di durata*, in AA.VV., *Conformazione del contratto e Autorità indipendenti nel diritto italo-europeo*, *Atti del* 16°*Convegno Nazionale SISDiC*, Napoli, 2023, pp. 199 ss., il quale osserva che «le conciliazioni sono affidate di regola a funzionari della stessa Autorità e che i componenti dei collegi arbitrali si trovano designati da queste e vi operano attraverso i loro uffici e valendosi di personale che le medesime Autorità mettono a disposizione. Fa poi specie rilevare come quei collegi si trovino ad applicare regole procedurali e non di rado anche sostanziali che le stesse hanno deliberato. Le regole del giusto processo – ripeto di là da ogni considerazione, che sarebbe superflua, sulla qualità delle decisioni o sulla riuscita delle conciliazioni – pone più di un problema con riguardo all'autonomia e all'indipendenza di questi organismi e quindi di nuovo sull'effettività della tutela assicurata alle parti svantaggiate del mercato».

[48] V. TONDI DELLA MURA, *Poteri privati e diritti dei consumatori: la questione della mancata retroattività della legge civile a tutela del legittimo affidamento in un caso surreale di "zona d'ombra" all'accesso della giustizia costituzionale*, in *Federalismi.it*, 2023, pp. 117 ss.: «E nello scarto fra le grandi garanzie unionali, costituzionali e codicistiche, da un lato, e le specifiche legislazioni di settore, dall'altro, che si registrano i disagi e le incertezze della difficile tutela dei diritti dei consumatori. Sicché e nelle aule dei Tribunali e nelle affollate udienze di merito, che la *coraggiosa* resistenza costituzionale del consumatore deve (avere la fortuna di) incrociare l'altrettanto *coraggiosa* sensibilità costituzionale dei giudici *a quibus* (soprattutto non togati), di assumere il difficile impegno professionale della stesura dell'ordinanza di rimessione al giudizio della Consulta; prospettiva, questa, che presuppone un capitale umano non sempre a disposizione. E cosi, per inciso, viene in mente l'amara riflessione di Mario Bertolissi a proposito degli esiti forensi derivanti dall'avvento di un'intelligenza artificiale già incipiente: "nell'illustrare il divenire di talune professioni liberali: in primis, dell'avvocatura, ci si sofferma sugli studi internazionali, che si occupano di transazioni planetarie, dimenticando che, i più, sono altri; vale a dire, i milioni e milioni di persone, che avranno bisogno di un avvocato qualunque, che ha avuto come maestri Demostene e Cicerone, non un avvocato d'affari. E in atto la commedia degli equivoci, che è ostile – ove si guardi oltre l'apparenza –, innanzi tutto, alla Costituzione"».

[49] Cfr. la prospettiva di A. PISANI TEDESCO, *Strumenti privatistici per la sostenibilità ambientale e sociale*, Torino, 2024, pp. 2 ss. Qui si rileva che «In ambito giuridico, sia nelle risoluzioni programmatiche che nei prodotti di "legge dura", si consolida l'attenzione per l'ambiente e si nota un'enfasi quasi ossessiva su parole d'ordine che sembrano avere un portato taumaturgico, evocate ormai ad ogni piè sospinto, sebbene non sempre a

Il terzo omino impara così il grande insegnamento lasciato da Wells nella Guerra dei mondi: «Gli uomini infinitamente compiaciuti di sé stessi, percorrevano il globo in lungo e in largo dietro alle loro piccole faccende, tranquilli nella loro sicurezza d'esser padroni della materia»[50].

proposito: "sostenibilità", "economia circolare", "neutralità climatica", "fattori ESG" (acronimo di *Environmental*, *Social and Governance*)».

[50] H.G. WELLS, *La guerra dei mondi*, Londra, 1897.

Nazzaro AC, 'La tutela dei dati biometrici tra GDPR e AI ACT' (2024) 2 EJPLT, 37 – 53.
DOI: https://doi.org/10.57230/EJPLT242ACN

EJPLT
ISSN 2704-8012



La tutela dei dati biometrici tra GDPR e AI ACT

The protection of biometric data between the GDPR and the AI ACT

ANNA CARLA NAZZARO
Professore Ordinario di Diritto Privato
Università degli studi Internazionali di Roma

Abstract

Il saggio analizza la tutela dei dati biometrici nell'ambito del GDPR e dell'AI ACT, evidenziando il delicato equilibrio tra protezione della privacy e innovazione tecnologica. Viene esaminata la definizione di dato biometrico e il suo utilizzo per identificazione, autenticazione e categorizzazione, con particolare attenzione ai rischi legati alla discriminazione e all'uso improprio. Si affrontano i divieti di raccolta indiscriminata e le implicazioni etiche dell'impiego dell'IA nel riconoscimento facciale e nell'analisi delle emozioni. Infine, si discute il ruolo della valutazione d'impatto e la necessità di un approccio regolatorio che tuteli i diritti fondamentali.

The essay explores the protection of biometric data within the framework of the GDPR and the AI ACT, highlighting the delicate balance between privacy protection and technological innovation. It examines the definition of biometric data and its use for identification, authentication, and categorization, with a focus on the risks of discrimination and misuse. The paper addresses the bans on indiscriminate data collection and the ethical implications of AI in facial recognition and emotion analysis. Finally, it discusses the role of impact assessment and the need for a regulatory approach that safeguards fundamental rights.

* Questo articolo è stato presentato alla ReCEPL Annual Conference "Diritto privato e sviluppo tecnologico sostenibile: le nuove categorie tra Italia e Argentina", 21 ottobre 2024, Università degli Studi Suor Orsola Benincasa.

© The author(s) 2024, 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: Dati biometrici; identificazione biometrica; Bias algoritmico; riconoscimento facciale

Summary: 1. Definizione di dato biometrico. – 2. Segue: Identificazione univoca della persona. – 3. Identificazione, autenticazione e categorizzazione. – 4. Dal rilevamento biometrico al rilevamento delle emozioni. – 5. Dati biometrici e personalità dell'individuo. – 6. Qualità del dato, pericolo di *bias* e valutazione d'impatto.

1. Definizione di dato biometrico.

La definizione di dato biometrico necessita di essere distinta da altre definizioni (come, ad esempio, quella di dato sanitario) ed è fondamentale determinarne l'autonomia rispetto al concetto di dato personale.

A tal fine è d'obbligo partire dalla normativa, denominata comunemente AI ACT (Reg. 2024/1689/UE) [1], che si occupa di stabilire regole uniformi sull'intelligenza artificiale e di sviluppare un ecosistema di fiducia attraverso un quadro giuridico per un'IA affidabile[2].

L'AI ACT, nella versione pubblicata in GU dell'UE il 12 luglio 2024 e che sarà applicabile in maniera parziale, a decorrere dal 2 febbraio 2025, all'art. 3, n. 34, in tema di definizioni, si appresta a qualificare dati biometrici i «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici».

Questa formulazione, che riprende quasi pedissequamente la definizione già contenuta nel Reg. 2016/679/UE (GDPR)[3], acquista un rilievo centrale nel tema che si sta trattando poiché aiuta a delimitare la nozione creando una

[1] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, 13.06.2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti 300/2008/CE, 167/2013/UE, 168/2013/UE, 2018/858/UE, 2018/1139/UE e 2019/2144/UE e le direttive 2014/90/UE, 2016/797/UE e 2020/1828/UE (regolamento sull'intelligenza artificiale).

[2] L'obiettivo è ripreso anche dalla Commissione europea nel *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65), 19.02.2020.

[3] La definizione, infatti, è conforme a quella contenuta nell'art. 4, punto 14, GDPR: «dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici». La definizione contenuta nel GDPR è, dunque, più specifica rispetto a quella contenuta nell'AI ACT anche se, come si vedrà, l'identificazione del soggetto è necessaria anche nell'ambito di quest'ultimo sistema di norme. Ulteriori definizioni sono contenute nell' art. 3, n.13, Direttiva 2016/680/UE del Parlamento europeo e del Consiglio, 27.04.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, la quale lì indica come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»; ripresa pedissequamente nell'art. 5, n. 18 del Regolamento 2018/1725/UE del Parlamento europeo e del Consiglio, 23.10.2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

correlazione di *genus ad speciem* tra dati biometrici e dati personali[4] allorché si afferma che i primi sono una particolare tipologia di dati personali[5]. E la specificità sta nel processo di estrazione che deve essere un trattamento tecnico specifico, relativo alle caratteristiche di una persona. Non, dunque, la caratteristica in sé (che altrimenti sarebbe dato personale), ma quella caratteristica isolata e resa fruibile in un certo modo da uno specifico trattamento tecnico.

Essa, peraltro, non è una inutile puntualizzazione perché, l'individuazione di quale debba essere il trattamento che consente di accedere alla nozione di dato biometrico, e dunque all'applicazione di una disciplina molto scrupolosa e restrittiva[6], non è di poco conto ed è già stata oggetto di pronunce da parte di autorità di controllo.

L'esempio che viene subito alla mente è il noto caso di Clearview AI[7], la società statunitense la cui attività è stata sanzionata da diversi garanti degli Stati europei[8] per violazione del GDPR. Ma ciò che qui interessa è il funzionamento della tecnologia di Clearview AI che si basa sulla disponibilità di un (enorme) database di immagini di persone, creato dalla società attraverso lo *scraping* di immagini via web e relative informazioni[9]. Dalle immagini si ottengono rappresentazioni vettoriali del volto che riproducono le caratteristiche identificative delle persone[10], rappresentazioni poi indicizzate

[4] La necessità di coordinamento tra le due discipline è messa in risalto da D. IACOVELLI, M. FONTANA, *Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici*, in *Il diritto dell'economia*, 2022, III, 107-138; G. CERRINA FERONI, *Intelligenza artificiale e ruolo della protezione dei dati personali*, intervento a Key4biz 14.02.2023; G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, V, 1193-1213.

[5] Con ciò non si vuole comunque affermare che l'una sia generale e l'altra speciale poiché entrambe sono dirette a tutelare valori attinenti alla persona umana. Per queste riflessioni cfr., C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di Bio Diritto*, 2021, III, 415-437.

[6] La regolamentazione dei dati biometrici è oggi contenuta in numerosi atti normativi. Oltre al già citato GDPR, si segnalano la Direttiva 2016/680/UE sulla protezione dei dati per le autorità di polizia e di giustizia penale (Direttiva LED), il Regolamento 2018/1725/UE, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati e la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 1981 aggiornata nel 2018. Sono poi fornite differenti definizioni di dati biometrici da: Comitato Nazionale per la Bioetica (CNB), *L'identificazione del corpo umano: profili bioetici della biometria*, 2010, 3, consultabile al *link https://bioetica.governo.it/it/pareri/pareri-e-risposte/l-identificazione-del-corpo-umano-profilibioetici-della-biometria/*; Gruppo di lavoro WP193 — Articolo 29 per la tutela dei dati personali, parere 3, 27.04.2012, consultabile al link *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec6;* Garante per la protezione dei dati personali, la quale, *Linee guida in materia di riconoscimento biometrico e firma grafometrica,* 2014, consultabili al seguente *link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3132361*.

[7] Sul quale v., F. LALA, *Data collection via web scraping: privacy and facial recognition after Clearview*, in *i-lex Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, Vol. 16, II, 2023, 34 - 45.

[8] Il progetto è stato anche al centro di casi giurisprudenziali soprattutto statunitensi: cfr, Circuit Court of Cook County, Illinois, May 28, 2020, No. 9337839, citata da F. LALA, *Data collection via web scraping: privacy and facial recognition after Clearview*, cit., 40 ss., ove anche una rassegna delle decisioni dei Garanti europei.

[9] Sul funzionamento specifico cfr. P DAUVERGNE, *Identified, Tracked, and Profiled*, Cheltenham, 2022. 59 - 68.

[10] Su tali tecniche cfr., E. SACCHETTO, *Brevi riflessioni sui fondamenti e limiti del rapporto fra automated faced-based human recognition technology e procedimento penale*, in *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. II, *Amministrazione, responsabilità, giurisdizione*, a cura di A. PAJNO, F. DONATI, A. PERRUCCI, Bologna, 2022, 541 ss., cui si rinvia per una sintetica ed efficace spiegazione del funzionamento del riconoscimento facciale tramite *software*; in argomento v. anche L. ALGERI, M. TORRE, *Aspetti definitori e delimitazione della materia*, in *La decisione penale tra intelligenza emotiva e intelligenza artificiale*, a cura di G.M. BACCARIM, P. FELICIONI, Milano, 2023, 96 ss.

in modo da permetterne l'utilizzo come motore di ricerca: il matching è semplice, basta avere l'immagine della persona che si vuole cercare (trasformata anch'essa in un modello vettoriale) e compararla con i modelli indicizzati nel database. Per fare ciò Clearview adotta un algoritmo di machine learning per la creazione e comparazione dei modelli.

Il caso in oggetto che come noto costituisce uno dei primi casi presi in considerazione da Autorità Garanti, rappresenta proprio un indicatore per la definizione di dato biometrico poiché sicuramente le fotografie di persone fisiche non possono essere considerate *tout court* come dati biometrici ai sensi della definizione del GDPR (ripresa dall'AI ACT[11]), in quanto è necessario un «trattamento tecnico specifico». Nel caso di Clearview, quindi, le immagini di persone fisiche identificabili (e i metadati associati) contenute nel *database* "raschiato" dal web sono dati personali, ma non biometrici. Diventano dati biometrici quando ad essi viene applicato il trattamento vettoriale che permette di ottenere il modello delle immagini nel database e dell'immagine sonda da sottoporre a comparazione[12]. Solo all'esito di questo processo possiamo essere sicuri di essere in presenza di dati biometrici.

2. Segue: Identificazione univoca della persona.

Dal confronto tra la definizione adottata dal GDPR e quella dell'AI ACT emerge tuttavia un altro elemento necessario alla definizione e cioè la possibilità di identificazione univoca di una persona.

Tale conclusione è stata di recente ribadita dalla Corte di Cassazione che in un noto caso che vedeva coinvolto un Istituto universitario ha confermato la sanzione del Garante Privacy affermando il principio di diritto secondo cui «In tema di trattamento dei dati personali, ai sensi dell'art. 9 del GDPR, ricorre un trattamento di dati biometrici, come definiti dall'art. 4, n.14 dello stesso Regolamento, quando i dati personali sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un software che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da un elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica»[13].

---

[11] Non è questo l'unico punto di contatto tra le due normative, anzi nell'ambito dell'AI ACT è palesemente indicato che la sua applicazione non pregiudica quella del GDPR. Per queste riflessioni v., P. FALLETTA E A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Riv. It. Inf. dir.*, 2024, I, 1-19.

[12] Per queste riflessioni cfr., Garante per la protezione dei dati personali, *Verifica preliminare. Sistema di rilevazione delle immagini dotato di un software che permette il riconoscimento della persona (morfologia del volto)*, 15.03.2018, n. 155, ove si specifica che «nel caso del riconoscimento facciale, il presupposto perché il trattamento delle immagini possa essere qualificato come trattamento biometrico è che i confronti finalizzati al riconoscimento dell´individuo (verifica dell´identità, nel caso in esame) siano automatizzati mediante l´ausilio di appositi strumenti software o hardware (che non sussistono nel caso di specie».

[13] Cass. Civ., sez. I, 13.05.2024, n. 12967 che ha cassato con rinvio la decisione di Trib. Milano, 20.10.2022, n. 8174, con la quale il Tribunale aveva accolto il ricorso di un istituto universitario avverso un provvedimento

Dunque, per accedere alla nozione, e alla disciplina, del dato biometrico c'è anche da verificare la nozione di identificazione biometrica [14] ossia il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati.

In realtà, già sotto il vigore del solo GDPR, il dato biometrico è sempre stato legato indissolubilmente alla individuazione univoca di una persona fisica e lo stesso AI ACT, richiamando l'art. 4, punto 14, del GDPR, mostra di non volersi discostare da tale nozione[15].

Del resto, oltre a tutta la dottrina unanime sul punto, anche se non sempre con una motivazione ben definita, già l'EDPB, nelle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video [16], al punto 76, evidenziava alcune componenti qualificanti nella definizione e nel trattamento dei dati biometrici, sulla base della definizione all'articolo 4 e per l'applicazione dell'art. 9 del GDPR. In particolare, altre alla «natura dei dati», che devono essere relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e ai «mezzi e modalità del trattamento» per cui i dati devono essere ottenuti da un trattamento tecnico specifico, si poneva l'accento sulla «finalità del trattamento», ossia l'identificazione univoca della persona.

Dunque, il dato biometrico che interessa ai nostri fini era già unanimemente considerato dalla dottrina e dal legislatore come quello che consente una correlazione tra dato biologico-fisico e identificazione univoca della persona[17],

---

del Garante privacy (n. 317 del 16 settembre 2021) che aveva individuato la violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 9, 13, 25, 35, 44 e 46, del Regolamento, nonché 2-*sexies* del Codice, per aver utilizzato un sistema di rilevamento del volto degli studenti durante esami a distanza al fine di controllarne la regolarità. Secondo il Garante il consenso espresso dagli studenti non poteva reputarsi una valida base giuridica del trattamento perché non avrebbe rappresentato una "manifestazione di volontà libera" (art. 4, par. 1, n. 11) del Regolamento), in ragione dello squilibrio della posizione degli studenti rispetto al titolare del trattamento (cfr. considerando n. 43 del Regolamento). Il Tribunale aveva confutato il ragionamento del Garante negando *in nuce* la classificazione del dato come biometrico, poiché nel caso di specie si sarebbe trattato di una semplice comparazione di immagini fotografiche, mentre affinché occorra la fattispecie di trattamento di dati biometrici sarebbe stato necessario che da una foto o da un video si ricavino caratteristiche biologiche per derivarne un modello matematico del volto del soggetto ritratto, a fini di riconoscimento. Ciò che mancava, a detta del Tribunale, nel caso concreto, era la finalità di identificazione. La Cassazione, invece, disattende tale conclusione poiché riconosce nel complesso sistema tendente ad individuare comportamenti anomali integra un autonomo e articolato trattamento dei dati biometrici acquisiti ed elaborati dallo stesso software, e attiene anche alla conferma dell'identità della persona fisica esaminata.

[14] Già nel 2014, l'allegato A del Provvedimento generale prescrittivo in tema di biometria, che definisce le Linee-guida in materia di riconoscimento biometrico e firma grafometrica, Allegato al Provvedimento del Garante per la Protezione dei dati personali, 12.11.2014, distingueva tra dato biometrico e identificazione, specificando che il procedimento di identificazione consiste nella «ricerca in un archivio, per confronto biometrico, di uno o più modelli biometrici corrispondenti al dato acquisito».

[15] L'esigenza di coordinamento è molto sentita dallo stesso legislatore dell'AI ACT che al considerando 7 avverte come la definizione debba essere interpretata conformemente a («*in light of* ») quella fornita dal GDPR e dalle direttive di settore.

[16] Comitato europeo per la protezione dei dati, Linee guida sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, 29.01.2020, n. 3, disponibili al seguente link: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf.

[17] In questo, già GDPR, art. 4, n. 14. Cfr., anche l'interpretazione della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, che già nel 1981 all'art. 6 vietava il trattamento automatico dei dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale.

ciò indipendentemente dal concetto di "identificazione biometrica" poi introdotto nel n. 35 del medesimo art. 3 dell'AI ACT e definito come "riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati". Infatti, le definizioni fornite nei riferimenti normativi fin'ora presi in considerazione contengono già *in nuce* il concetto di identificazione univoca[18].

Si deve però aggiungere che tale apparente perdita di centralità di questo concetto di identificazione nella definizione fornita dall'AI ACT, non deve essere inteso come irrilevanza di esso, anzi sembra rappresentare una rinnovata autonomia del requisito.

3. Identificazione, autenticazione e categorizzazione.

Sia chiaro comunque che identificazione non è autenticazione, ciò per espressa affermazione dello stesso considerando n. 15 che esclude dalle ipotesi di identificazione biometrica «i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali».

In questo senso, dunque, i sistemi che permettono di sbloccare gli smartphone con il volto o con le impronte digitali[19] non sono dati biometrici ai fini della normativa eurounitaria[20]. La distinzione non è nella modalità di rilevamento, ma nelle modalità di trattamento del dato e in particolar modo nel confronto di quel dato con un'entità di paragone laddove nel caso di autenticazione si opera un singolo confronto con un modello predefinito conservato nel dispositivo, nel caso invece di identificazione il confronto è più ampio e più invasivo e rischioso per la persona ed è relativo a banche dati esterne al sistema di riconoscimento.

[18] I problemi dell'identificazione biometrica sono soprattutto quelli legati alla possibilità di errore tanto che l'AI Act vieta l'identificazione biometrica remota «in tempo reale» che si verifica nei casi in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono contestualmente.

[19] La Corte europea dei diritti dell'uomo si è in vario modo occupata di tutelare i dati biometrici e, in particolar modo le impronte digitali (McVeigh, O'Neill and Evans v. the United Kingdom, 1981; Kinnunen v. Finland, 1993; S. and Marper v. the United Kingdom [GC], 2008; Dimitrov-Kazakov v. Bulgaria, 2011; M.K. v. France, 2013; Suprunenko v. Russia (dec), 2018; Gaughran v. the United Kingdom, 2020; P.N. v. Germany, 2020); Willems v. the Netherlands (dec.), 2021), o il timbro vocale (P.G. and J.H. v. the United Kingdom, 2001; Allan v. the United Kingdom, 2002; Doerga v. the Netherlands, 2004; Vetter v. France, 2005; Wisse v. France, 2005).

[20] In tal senso si era espresso anche il Garante per la Protezione dei dati personali italiano nel Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014. In un'altra interessante decisione (Garante per la protezione dei dati personali, *Installazione di apparati promozionali del tipo "*digital signage*" (definiti anche Totem) presso una stazione ferroviaria*, 21.12.2017) il Garante ha distinto tra "*face detection*", intesa come mero rilevamento del volto e "*face recognition*", ossia identificazione della persona, questa distinzione corrisponde a quella tra dati personali e dati biometrici.

Ovviamente anche nel caso di autenticazione si pongono problemi di tutela dei dati, poiché essi sono comunque come dati personali[21], ma non si reputa applicabile la disciplina più stringente prevista per i dati biometrici.

L'importanza centrale che assume nella definizione del dato biometrico lo scopo per cui si attua il trattamento diventa ancor più chiara con la nozione di "categorizzazione biometrica" di cui al 16 considerando e, all'art. 3, n. 40, come un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche[22]. In questa ipotesi, dunque, il medesimo rilevamento delle caratteristiche fisiologiche del soggetto è destinato alla creazione di categorie[23].

Appare chiaro, dunque, che la distinzione tra le definizioni riportare e fornite dall'AI ACT non risiede nella modalità di rilevamento dei dati, ma dalla finalità e dalle modalità del trattamento e, in particolar modo sembra che, stante la caratteristica di trattamento tecnologico delle fattezze dell'individuo, che serve a distinguere tale rilevamento dal semplice ritratto (sia esso anche fotografico), si possa discorrere di dato biometrico soltanto ove si sia in presenza di una identificazione della persona. Per vero, le sole norme analizzate non permettono immediatamente di raggiungere tale conclusione, potendosi immaginare tanto per l'autenticazione, quanto per la categorizzazione sistemi che sommano ad esse l'identificazione. Quest'ultima invece assume il ruolo di requisito dalla lettura congiunta, richiesta anche dall'AI ACT, delle norme del GDPR.

E, in questa prospettiva, l'AI ACT aggiunge una particolare attenzione alla finalità del trattamento la cui liceità non deriva più dal solo consenso dell'interessato, ma dal rispetto della normativa definita per quella particolare operazione. In altri termini, ciò che può essere lesivo della persona è la finalità del trattamento, cioè come viene trattato il dato e a quale scopo[24].

---

[21] Per queste riflessioni v., L. GRECO E A. MANTELERO, *Industria 4.0, robotica e* privacy-by-design*,* in *Dir. inf. e informatica*, 2018, VI, 875 - 900.

[22] Sul concetto di categorizzazione v., G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 35, il quale la definisce come un procedimento «consistente nell'estrarre le caratteristiche dall'immagine di una persona (conosciuta o meno) al fine di classificarla in una o più categorie in base agli attributi [come] età, sesso, abitudini di consumo». Significativo è l'esempio riportato delle consolle di gioco in grado, in alcuni casi, di categorizzare anche l'umore del giocatore.

[23] Sulle problematiche relative alla profilazione attraverso l'utilizzo di dati biometrici, v., P. PACILEO, *Profilazione e diritto di opposizione*, in Aa.Vv., *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, 179, che pone in risalto come gli strumenti di profilazione utilizzino sempre più le potenziali capacità individuali, relazionali, motivazionali ma anche individuando i gradi di soddisfazione personale, creando profili comportamentali dinamici di clienti per realizzare un'offerta mirata.

[24] In questo senso l'Autority canadese che si è occupata del caso Clearview ha utilizzato la locuzione "scopo inappropriato": Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta.

Forse questo è il passaggio ulteriore che, pur nel collegamento con il GDPR caratterizza l'AI ACT, neutrale dal punto di vista dei dati[25], ma interessato all'obiettivo per cui sono utilizzati[26].

In questo senso, il dato biometrico che può astrattamente essere utilizzato ai fini di identificazione e categorizzazione, rileva nella sua caratteristica di dato personale particolare, quando tale identificazione o categorizzazione permette l'identificazione della persona ed è utilizzata per finalità che possono reputarsi pericolose o lesive della dignità personale[27].

Tra gli scopi considerati pericolosi rientra (ed è dunque vietato) l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso, che potrebbe creare un sistema di controllo di massa[28]. Tale divieto deriva dalla lettura congiunta di GDPR e AI ACT, che consente di desumere dalla interpretazione delle regole di entrambe le normative una disciplina molto restrittiva per tali dati biometrici con dei divieti specifici tra i quali, a norma dell'art. 5, anche la raccolta indiscriminata ("*untargeted scraping*") di immagini facciali allo scopo di creare o ampliare *database* di riconoscimento facciale[29].

---

[25] La scelta politica alla base della formulazione dell'AI ACT è stata quella di emanare un regolamento generale ed orizzontale, diretto a disciplinare il fenomeno dell'intelligenza artificiale senza tuttavia entrare troppo in tecnicismi che avrebbero condotto ad una rapida obsolescenza delle norme. In aggiunta, l'obiettivo degli organi dell'Unione era anche quello di rendere il modello europeo un riferimento globale atto ad essere implementato in tutto il resto del mondo, definendo regole applicabili con facilità in altri sistemi. Per queste riflessioni v., P. FALLETTA E A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR* , cit., 3.

[26] In questo senso, un ulteriore punto di contatto tra le due norme è l'approccio basato sul rischio che impone un comportamento di compliance al privato. Sul punto v., F. PIZZETTI, *GDPR e Intelligenza Artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in AA.VV., *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna, Studi in tema di Internet Ecosystem*, a cura di A. MANTELERO, D. POLETTI, Pisa, 2018, 69 - 97. E trova anche A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, IV, 1239-1260.

[27] Tra le possibilità di lesione si ritrova anche la decontestualizzazione degli individui, nel senso che il soggetto potrebbe essere preso in considerazione soltanto per alcuni degli aspetti rilevati e non per la sua totale personalità. Per queste considerazioni v., G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 23 ss., che afferma come ciò può risolversi in una rappresentazione parziale e fuorviante della persona. Si aggiunga che il sistema del riconoscimento biometrico rende più netta la distinzione tra identificazione e identità poiché le fattezze biometriche sono normalmente decontestualizzate. Per queste riflessioni v., Gruppo di lavoro articolo 29, *Parere sugli sviluppi nelle tecnologie biometriche*, 27.04.2012, n. 3, 6, disponibile al link: https://www.garanteprivacy.it/documents/10160/2150354/wp193.pdf, che chiarisce come la prima consiste nel confronto dei dati biometrici della persona con una serie di modelli biometrici conservati in una banca dati mentre la seconda consiste nel confronto con un unico modello biometrico conservato in un dispositivo; Il tema era stato già affrontato dal Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria*, 26.11.2010, 14 ss., che addirittura discorre del corpo umano come password, chiarendo con ciò la limitata utilizzazione degli strumenti di autenticazione biometrica.

[28] Tale controllo è verosimile soprattutto a fronte di sistemi politici meno improntati ai valori espressi nella nostra Carta costituzionale come, ad esempio, quello cinese dove esiste un "*Social Credit System*" attraverso il quale ogni cittadino riceve in modo automatizzato un punteggio di affidabilità. La circostanza è denunciata da G. MOBILIO, Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative, cit., 11 ss. e 208 ss., il quale mette anche in evidenza la particolare pericolosità per la libertà dell'individuo delle tecnologie di riconoscimento facciale.

[29] Il percorso seguito dall'AI ACT non è stato tuttavia lineare. Infatti, soprattutto con riferimento ad alcune utilizzazioni delle tecniche di riconoscimento facciale, in particolare con riferimento al riconoscimento delle emozioni facciali, si è passato da un divieto assoluto ad una soluzione più mite. Per tali riflessioni v., M.

Si tratta della nota tematica del divieto di *webscraping*[30] e la necessità di spiegarne la ratio ove il legislatore pur ammettendo l'uso, anche se a certe condizioni di dati biometrici, vieta il *webscraping* di essi.

Per risolvere la questione sembra necessario puntare l'attenzione proprio sulle finalità del trattamento poiché il problema è che quando si raschiano dati personali dal web [31], la liceità del loro utilizzo può dipendere, e anzi necessariamente deve dipendere, dalla finalità della raccolta. La norma non vieta *tout court* lo *scraping*, ma la creazione o l'ampliamento tramite esso di banche dati di riconoscimento facciale.

Tale previsione è assolutamente in linea con il GDPR poiché l'art. 6, considera le basi giuridiche sempre in ragione del particolare contesto e della specifica finalità del trattamento. Così altro è il *webscraping* finalizzato ad addestrare l'AI[32], altro è quello utilizzato per ragioni di pubblica sicurezza, altro è quello utilizzato per ragioni commerciali e così via.

Di ciò è ben conscio il nostro Garante privacy, quando nelle linee guida del maggio 2024[33] «propone una diversa prospettiva, esaminando la posizione dei soggetti, pubblici e privati, gestori di siti *web* e piattaforme *online,* operanti quali titolari del trattamento di dati personali, che rendano pubblicamente disponibili, dati (anche personali) che vengono raccolti dai *bot* di terze parti». Tutto ciò nella consapevolezza che il funzionamento stesso del sistema di internet è basato su *web crawler,* cioè programmi che scandagliano sistematicamente il web al fine di raccogliere i dati contenuti nelle pagine web ed indicizzarli per garantire il funzionamento dei motori di ricerca.

Del resto, anche il comportamento illecito imputato nel noto caso Clearview AI non era tanto il *webscraping*, quanto l'utilizzo che si faceva dei dati rastrellati dalla rete[34].

Sembra a questo punto necessario rispondere ad una possibile obiezione e cioè che in fondo si tratterebbe di dati pubblici. L'obiezione sembra facilmente superabile oltre che per le ragioni oramai comunemente accolte dalla dottrina[35] anche perché il problema è la finalità dell'utilizzo di dati sensibili e il

---

MATTIOLI AND F. CABITZA, *Not in My Face: Challenges and Ethical Considerations in Automatic Face Emotion Recognition Technology*, in *Mach. Learn. Knowl. Extr.* 2024, VI, 2221.

[30] Per una definizione v., B. ZHAO, *Web Scraping*, in AA.VV., *Encyclopedia of big data*, a cura di L.A. SCHINTLER, C.L. MCNEELY, Cham, 2022, 951 - 953: «*Web scraping, also known as web extraction or harvesting, is a technique to extract data from the World Wide Web (WWW) and save it to a file system or database for later retrieval or analysis. Commonly, web data is scraped utilizing Hypertext Transfer Protocol (HTTP) or through a web browser. This is accomplished either manually by a user or automatically by a bot or web crawler*».

[31] Ciò deriva dal fatto che tutti i sistemi di AI riescono a funzionare soltanto se hanno a disposizione una enorme quantità di dati. G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.*, 2022, IV, 1085 - 1099; C. COLAPIETRO, A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal – Rivista di BioDiritto*, 2020, III, 359 - 387. Il fenomeno, già prima dell'avvento dei sistemi di AI aveva impegnato gli studiosi di Big Data. Cfr. A.C. NAZZARO, L'utilizzo dei Big data, cit.

[32] Su quest'ultimo si evidenziano problemi legati alla titolarità dei dati utilizzati. Cfr., A.M. PARK , *Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Data Scrapers Personal Information from Data Scrapers*, in *Michigan Law Review*, Vol. 120, V, 2022, 914 ss..; G. XIAO, *Bad Bots: Regulating the Scraping of Public Personal Information*, in *Harv. J.L. & Tech.,* Vol. 34, II, 2021, 702.

[33] Garante per la protezione dei dati personali, *Web scraping ed intelligenza artificiale generativa: nota informativa e possibili azioni di contrasto*, maggio 2024.

[34] La doppia valenza, in negativo e in positivo, degli strumenti di *webscraping* è evidenziata da F. LALA, *Data collection via web scraping: privacy and facial recognition after Clearview*, cit., 35.

[35] Oramai è generalmente accolta l'opinione che considera tutelati anche i dati pubblici nel rispetto della c.d. vita sociale privata. Cfr., L*ópez Ribalda and Others v. Spain* [GC], nos. 1874/13 and 8567/13, §§ 87-88, 17

Garante, proprio in questo documento di raccomandazione, non suggerisce ai gestori accorgimenti funzionali di evitare tout court il *webscraping* (che sarebbe un obiettivo irrealizzabile), ma individua possibili azioni di contrasto per fare in modo che tale *webscraping* sia utilizzato per finalità di addestramento della IA generativa in modo lecito.

4. Dal rilevamento biometrico al rilevamento delle emozioni.

Tra i divieti di utilizzo di dati biometrici giustificati non dal dato in sé ma dalla finalità del trattamento rientrano anche l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale, perché potrebbero essere fonte di discriminazioni basate su tali caratteristiche; l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione perché potrebbe essere considerato lesivo della libertà personale[36].

L'ipotesi da ultimo riportata apre la strada ad ipotesi ulteriori di rilevamento di caratteristiche fisiologiche, non strettamente fisiche che sono caratterizzate da una invasività maggiore sul corpo e sulla psiche dell'individuo. Tali casi sono stati già oggetto di valutazione da parte di autorità di controllo. Ad esempio l'Autorità nazionale per la protezione dei dati e la libertà d'informazione ungherese [37] ha censurato il comportamento di un istituto finanziario che analizzava le telefonate registrate dal servizio clienti e, tramite un sistema di *machine learning,* individuava lo "stato emozionale" della conversazione sulla base della voce, delle pause e del numero delle persone intervenute, con lo scopo di selezionare i clienti particolarmente insoddisfatti, da richiamare, per prevenire future lamentele e migliorare in generale i processi interni di gestione.

Anche in questa ipotesi, se oggi il problema può essere quello di definire i dati trattati in termini di dati biometrici o meno, all'esito dell'AI ACT, all'epoca dei fatti era quello di tutelare i soggetti coinvolti, utilizzando le norme in quel momento a disposizione, e l'Autority ungherese, utilizzando il GDPR e pur non qualificando i dati in questione come biometrici, perché non consentivano l'identificazione univoca della persona, ha considerato illegittimo il trattamento effettuato perché l'impresa non aveva provveduto ad informare adeguatamente gli interessati sui trattamenti effettuati, secondo un principio di trasparenza analogo a quello su cui è basata la disciplina dei «sistemi di riconoscimento delle emozioni» nel regolamento AI ACT[38].

October 2019; *Nikolay Sergeyevich Glukhin v. Russian Federation*, App no. 11519/20 (ECtHR, 4 July 2023), commentata da M. ZALNIERIUTE, *Glukhin v. Russia. App. No. 11519/20. Judgment*, in *American Journal of International Law*, Vol. 117, IV, 2023, 695 - 701.

[36] In quest'ultima ipotesi si tratta di un sistema di IA «finalizzato all'identificazione o alla deduzione di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici».

[37] Nemzeti Adatvédelmi és Információszabadság Hatóság, 8.02.2022, n. 85-3/2022, in https://www.naih.hu/hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei.

[38] Tali tecniche rientrano, a norma dell'art. 5, tra le pratiche vietate ove siano utilizzate nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in

La pericolosità di questi sistemi di rilevamento delle emozioni per i diritti e le libertà delle persone può essere amplificata da utilizzazioni tese ad implementare strumenti predittivi e ciò anche muovendo da utilizzi che invece appaiono non soltanto leciti, ma anche auspicabili.

Le utilizzazioni più frequenti, sono proprio quelle ammesse dall'AI ACT che godono dell'eccezione dal divieto perché utilizzate per pubblica sicurezza e, in particolar modo, le tecniche dirette a garantire la sicurezza transfrontaliera. Tale tema è fortemente avvertito dal legislatore eurounitario tanto che si sono succeduti anche Regolamenti destinati a disciplinare l'utilizzo di dati biometrici alle frontiere [39]. In particolare, il Regolamento 2226/2017/UE istituisce un "sistema di ingresso/uscita" (EES), che registra e memorizza la data, l'ora, il luogo di ingresso e di uscita, nonché i dati biometrici dei cittadini di paesi terzi, con l'obiettivo di "Aumentare la sicurezza delle frontiere utilizzando tecnologie moderne, come l'intelligenza artificiale e le tecniche biometriche. Le norme contenute in tale regolamento sono di stringente applicazione tanto che dal necessario coordinamento con quanto previsto dalla Direttiva 2016/680/UE[40], che all'art. 10 richiede un consenso rafforzato per l'utilizzazione di dati biometrici anche da parte delle forze dell'ordine, deriva che il loro trattamento è «autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: *a*) se autorizzato dal diritto dell'Unione o dello Stato membro; *b*) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; *c*) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato».

In questa specifica applicazione, appare significativa una decisione della High Court of Justice gallese che nel 2019[41] ha affrontato il caso della legittimità dell'utilizzo da parte delle forze dell'ordine di un sistema di *Artificial face recognition* denominata AFR Locate [42]. La Corte, dopo aver riconosciuto

funzione o immesso sul mercato per motivi medici o di sicurezza e sono sottoposte, a norma dell'art. 50, a particolari obblighi di trasparenza. Ove ammesse, tali pratiche, sono comunque catalogate "ad alto rischio".

[39] Ad esempio il Regolamento 2022/991/UE, che modifica il Regolamento 2016/794/UE, si occupa di stabilire un'eccezione alle restrizioni riguardanti il trattamento automatizzato di dati biometrici intesi a identificare in modo univoco una persona, per consentire ad EUROPOL di prevenire e combattere la criminalità organizzata. Per questi dati v., V. VASTA, *Diritto dell'unione europea e intelligenza artificiale. Riflessi sul procedimento penale*, in *Riv. It. Dir. Proc. Pen.*, Vol. 67, I, 2024, 271 - 285.

[40] Relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

[41] Sentenza 4 settembre 2019, [2019] EWHC 2341, R (Bridges) c. CCSWP and SSHD.

[42] Il caso nasce da un progetto pilota che la polizia del Galles meridionale stava testando per l'intero Regno Unito, consistente nella raccolta di immagini digitali di volti ripresi in tempo reale in un contesto dinamico, confrontate con un database di soggetti sospettati o accusati di reati, in possesso delle forze dell'ordine. Nel caso in cui fosse avvenuto il *matching* e un operatore umano avesse confermato la correttezza della valutazione del software, le forze di polizia si sarebbero attivate per identificare il soggetto e procedere con la cattura o con la semplice segnalazione all'*intelligence.* Dato il numero di soggetti registrati e la sua ampia percentuale in considerazione della popolazione del Galles, la Corte si interroga sulla possibilità che il progetto integri gli estremi di un controllo di massa. Nonostante l'impiego dello strumento avvenisse in modalità esplicita, cioè avvertendo pubblicamente gli avventori della sua presenza, la Corte evidenzia che il trattamento dei dati personali non è assimilabile semplicemente ad un apparecchio fotografico installato in una pubblica piazza poiché viene analizzata l'informazione digitale che contiene l'immagine ne vengono estratti i dati facciali biometrici. Tale processo, a detta della Corte, sarebbe assibilabile ad una raccolta di impronte digitali o di DNA. Nonostante ciò, la Corte non reputa censurabile l'utilizzo dello strumento poiché rispetta sia l'art. 8 CEDU, sia le norme del GDPR. Per accurate riflessioni sulla sentenza v., A. PIN, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *DPCE on line*,

l'importanza di accordare l'uso di tali strumenti nel campo della tutela di interessi pubblici, afferma anche il necessario bilanciamento con la protezione dei diritti individuali [43], soprattutto per gli aspetti che gli stessi giudici definiscono "inquietanti" per la capacità di trattare enormi quantità di dati. Tuttavia, reputa legittimo l'uso dello strumento poiché risulterebbero correttamente utilizzati gli strumenti previsti dal GDPR per tutelare la privacy dei soggetti coinvolti[44].

Tuttavia, le tecniche atte a creare c.d. confini "intelligenti" potrebbero comprendere non solo l'uso di tecnologie biometriche a fini di identificazione, ma anche sistemi di rilevamento delle emozioni per individuare soggetti che potenzialmente siano non completamente sinceri riguardo a quanto dichiarato alla frontiera.

È proprio ciò che è accaduto nei casi di rilevamento delle emozioni alle frontiere. Si tratta di una evoluzione della tecnologia che ha prodotto anche strumenti di *Automatic Face Emotion Recognition* (FER), che sono dunque in grado di rilevare le emozioni, quantomeno quelle che modificano i dati biometrici[45].

Questi strumenti automatizzati di rilevamento degli inganni analizzano i dati biometrici di seconda generazione associati a stress, ansia e menzogna per supportare gli agenti di controllo delle frontiere. Sebbene non siano attualmente in funzione sistemi di rilevamento delle emozioni alle frontiere dell'UE, esiste un progetto, "*Intelligent Portable Control System*" (iBorderCtrl), che mira allo sviluppo di strumenti di rilevamento degli inganni e di strumenti di valutazione che, analizzando microespressioni, come ammiccamenti, aumento dell'arrossamento del viso o direzioni dei movimenti della testa, calcolano il rischio associato a ciascun soggetto. I sistemi iBorderCtrl mirano a identificare le persone che hanno mentito sulla loro identità, bagaglio, destinazione o altri piani di viaggio e classificano persone in viaggiatori "in buona fede" e "non in buona fede". Se una persona rientra in quest'ultima categoria, un funzionario di frontiera umano conduce un colloquio e ulteriori indagini[46].

2019, V, 3075- 3082. Per una rassegna della legislazione sul tema in Galles cfr., J. PURSHOUSE, L. CAMPBELL, *Automated facial recognition and policing: a Bridge too far?*, in *Legal Studies*, *Vol. 42, II,* 2022, 209 - 227.

[43] In questo senso non sembra sia accoglibile l'affermazione di chi reputa sicuramente giustificato l'uso di questi sistemi da parte delle forze dell'ordine e da verificare invece soltanto quando tale uso sia relativo a scopi commerciali. Cfr. B. MCNERNEY, Keep Your Fingerprints to Yourself: New York Needs a Biometric Privacy Law, in *St. John's Law Review*, 2022, Vol. 96, IV, 1039 - 1070.

[44] Un altro caso ha impegnato la Corte europea dei diritti umani (*Nikolay Sergeyevich Glukhin v. Russian Federation*, App no. 11519/20 (ECtHR, 4 July 2023) a seguito della contestazione di un cittadino russo che lamentava di essere stato sottoposto ad una tecnologia di riconoscimento facciale senza averne avuto notizia preventiva. In particolare, il ricorrente lamentava la violazione dell'art. 8 della Convenzione. Questo è stato il primo caso in cui la Corte ha affrontato i problemi legati all'uso di tale tecnologia ed ha espresso forti dubbi sul fatto che le disposizioni di legge nazionali che autorizzavano il trattamento dei dati personali biometrici, anche con l'ausilio della tecnologia di riconoscimento facciale, "in relazione all'amministrazione della giustizia" soddisfacessero il requisito della "qualità del diritto", poiché erano formulate in modo sommario e sembravano consentire il trattamento di tali dati in relazione a qualsiasi tipo di procedimento giudiziario. Il diritto nazionale, in altri termini, non conteneva limitazioni sulla natura delle situazioni che potevano dar luogo all'uso della tecnologia di riconoscimento facciale, sulle finalità previste, sulle categorie di persone che potevano essere oggetto di trattamento o sul trattamento di dati personali sensibili.

[45] Su questa tematica cfr., M. MATTIOLI AND F. CABITZA, *Not in My Face: Challenges and Ethical Considerations in Automatic Face Emotion Recognition Technology*, in *Mach. Learn. Knowl. Extr.* 2024, VI, 2201 - 2231.

[46] Il Progetto nasce dal finanziamento di un Programma Horizon ed è stato oggetto di decisioni del tribunale UE e della Corte di Giustizia dell'UE, 7 settembre 2023, C-135/22P, poiché un cittadino tedesco aveva chiesto

È palese che l'uso di questi sistemi di rilevamento biometrico dell'inganno è altamente rischioso poiché essi scontano una diversa caratterizzazione culturale delle modalità di esprimere, attraverso il volto, le proprie emozioni. Inoltre, essi non si fondano su solide basi scientifiche, ma piuttosto su una catena di ipotesi sulla relazione tra indicatori biometrici e intenzioni interne[47]. Uno dei problemi fondamentali di questi sistemi è che le emozioni sono fenomeni umani complessi che non possono essere chiaramente assegnati a un insieme di indicatori non verbali e verbali[48].

Ovviamente, anche tra i non giuristi, non mancano le obiezioni di chi reputa queste tecniche pericolose per le persone fisiche[49], soprattutto se si prende in considerazione la possibilità di errore[50] causato anche dalla presenza di *bias*[51].

5. Dati biometrici e personalità dell'individuo.

I problemi da valutare in ambito giuridico, tuttavia non sono solo quelli legati alla possibilità di errore dell'algoritmo.

---

il pieno accesso agli atti, negato dal Tribunale ed accolto parzialmente dalla Corte di giustizia (per la cui sentenza cfr., https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A62022CJ0135). La questione è efficacemente illustrata da F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in archiviopenale.it.

[47] Sul punto cfr., P. Grother, M. Ngan, K. Hanaoka, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects*, U.S. Department of Commerce, National Institute of Standards and Technology, 2019, disponibile sul sito web *www.nvlpubs.nist.gov* che riporta uno studio molto significativo condotto dal *National Institute of Standards and Technology* degli Stati Uniti, secondo il quale l'utilizzo di molti *software* di riconoscimento facciale è affetto da numerosi errori relativamente alle donne afroamericane e asiatiche; J. Della Torre, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in Aa.Vv., *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, a cura di G. Di Paolo, L. Pressacco, Napoli, 2022, 20 ss.. L'a. evidenzia come in questi casi non si tratti necessariamente di *bias*, ma del modo in cui sono costruiti gli algoritmi che sconta necessariamente difetti di selezione dei volti in fase di addestramento trasmettendo dunque alla macchina pregiudizi umani.

[48] Sul punto sono soprattutto le indagini di altre scienze a venire in soccorso. Cfr., M. Gendron, D. Roberson, J.M. van der Vyver; L.F Barrett, *Perceptions of emotion from facial expressions are not culturally universal: Evidence from a remote culture*, in *Emotion*, 2014, Vol. 14, II, 251 - 262.; J. Vincent, *Emotion Recognition Can't be Trusted*, in www.theverge.com, 2019; D. Matsumoto, *Cultural influences on the perception of emotion.*, in *J. Cross-Cult. Psychol.*, 1989, Vol. 20, I, 92 - 105.

[49] A. Katirai, *Ethical considerations in emotion recognition technologies: A review of the literature*, in *AI and Ethics*, 2024, Vol. 4, 927 - 948; K. Crawford, *Time to regulate AI that interprets human emotions*, in *Nature*, 2021, 592, 167 ss.

[50] La probabilità di errore è massima nelle ipotesi di *real time*, non a caso vietato dall'AI ACT, perché è stato provato che in queste ipotesi l'accuratezza dei tools può variare in modo significativo in base ad un'ampia gamma di fattori, come la qualità della fotocamera utilizzata, la luce, la distanza, la qualità dei dati immessi nel database (o dei dati ricavati dal flusso di video), o ancora l'etnia, l'età o il sesso del soggetto. Si deve tuttavia avvertire che il concetto di accuratezza utilizzato nel GDPR è differente dal medesimo concetto preso in considerazione nell'AI ACT laddove la prima normativa si riferisce all'accuratezza nella gestione dei dati, la seconda si occupa invece dell'accuratezza del risultato ottenuto dai dati processati. Per queste considerazioni v., C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, in *Computer Law & Security Review*, 2024, Vol. 55, 1-16.

[51] A. McStay, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, in *Big Data Soc.*, 2020, 7; T. Xu; J. White, S. Kalkan, H. Gunes, *Investigating bias and fairness in facial expression recognition*, in *Proceedings of the Computer Vision–ECCV 2020Workshops*, Glasgow, UK, 23-28 August 2020, Berlin/Heidelberg, 2020; 506 - 523; E. Kim, D. Bryant, D. Srikanth, A. Howard, *Age bias in emotion detection: An analysis of facial emotion recognition performance on young, middle-aged, and older adults*, in *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, Virtually, 19-21 May 2021, USA, 2021, 638 - 644; J. Buolamwini, T. Gebru, *Gender shades: Intersectional accuracy disparities in commercial gender classification*, in Proceedings of the *Conference on Fairness, Accountability and Transparency*, 23-24 February 2018, New York, 2018, 77 - 91.

Non si può dimenticare che i dati biometrici rappresentano una specificazione dei dati personali e sono dati sensibili ai sensi dell'art.9 del GDPR poiché rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, o ancora la salute o la vita sessuale o l'orientamento sessuale della persona[52]. Il loro trattamento è in principio vietato, tranne nel caso in cui si verifichi una delle condizioni previste dal secondo comma, tra cui rientra anche il consenso esplicito dell'interessato per una o più finalità specifiche (lett. a)[53], oppure nel caso in cui il trattamento risulti necessario per finalità stabilite dalla stessa norma[54].

Un caso specifico ha fatto molto scalpore proprio in Argentina dove, nell'agosto del 2023, l'Agenzia per l'accesso alla pubblica informazione (AAIP)[55] ha avviato un'indagine sulla liceità del trattamento dei dati personali da parte di una società di gestione di criptovalute, la Fondazione Worldcoin, la quale chiedeva ai clienti, dietro compenso in criptovaluta, di sottoporsi ad una procedura di scansione dei volti e delle iridi. Il problema riscontrato era la mancanza di una finalità dichiarata del trattamento[56]. La decisione dell'Autorità argentina di bloccare l'operazione commerciale si è fondata proprio sull'identificazione tra dato biometrico e dato sensibile[57].

Il progetto è, in realtà più ambizioso e avrebbe lo scopo di creare, proprio tramite la scansione dell'iride, che a detta degli studiosi sarebbe il dato biometrico più attendibile, una identità digitale per essere distinti con assoluta certezza da una AI.

Il problema è che le tecniche di rilevamento facciale collegate all'identità digitale, devono essere valutate nella consapevolezza del loro stretto rapporto con l'identità personale dell'individuo. In questo senso, nel progetto da ultimo riportato, la scansione del volto avrebbe reso possibile individuare la personalità di un individuo distinguendolo da una macchina, in quanto tale, senza personalità. Numerosi studiosi guardano con sospetto a queste tecniche

---

[52] Cfr. art. 9 co. 1. Infatti, i dati biometrici sono per gran parte strettamente identificativi della persona e contengono una impronta indelebile della persona. Per queste affermazioni cfr., S .EL SABI, *La tutela della* privacy *nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in *Dir. inf. e informatica*, 2023, V, 789 - 827. Lo stretto rapporto tra dati biometrici e personalità dell'individuo è rimarcata anche dal Gruppo di lavoro articolo 29, Parere sugli sviluppi nelle tecnologie biometriche, cit.

[53] In questo senso si è espressa Cass., Sez. Lav., 19.05.2023, n. 13873, in *Dir. § giust.*, che ha accolto la domanda di un lavoratore che chiedeva di dichiarare illegittimo un sistema di rilevazione biometrica, tramite impronta della mano, dell'accesso dei lavoratori da parte del datore di lavoro, perché il consenso prestato non era specifico. Tale consenso non esclude comunque limitazioni generali rispetto all'utilizzo di tali dati, tanto che il loro utilizzo quale corrispettivo di un servizio sarebbe da ritenersi in ogni caso sproporzionato. Così, G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf. e informatica*, 2020, III, 634 - 674.

[54] In particolare, il pericolo è di lesione di diritti personalissimi a causa di un potere incontrollabile che potrebbe derivare dalla tecnica dell'IA di processare questi dati personali. Cfr. L. STARK, J. HOEY, *The ethics of emotion in Artificial Intelligence systems*, in Proceedings of the 2021 ACM *Conference on Fairness, Accountability, and Transparency*, FAccT '21, 3 - 10 March 2021, New York, 782 - 793; Stark, L. The emotional context of information privacy. Inf. Soc. 2016, 32, 14–27; A. MCSTAY, *Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy*, cit., 7.

[55] Si tratta dell'equivalente dei Garanti privacy europei ed è l'Autorità esecutiva della legge 25.326 sulla protezione dei dati personali.

[56] Peraltro, è attualmente in discussione un progetto di legge per riformare profondamente la normativa in tema di dati personali che propone una specificazione maggiore anche delle finalità del trattamento.

[57] Il medesimo progetto è stato bloccato anche dalla Provincia di Buenos Aires che, tramite il Ministero della produzione, Scienza e Innovazione tecnologica, ha imposto una sanzione di 194 milioni di Pesos alla Worldcoin Foundation, perché non aveva previsto limiti di età alla partecipazione al progetto.

muovendo dall'assunto che il trattamento di dati biometrici può rivelarsi fortemente pericoloso, perché il volto sarebbe la finestra dell'anima [58] e, dunque, la sua scansione potrebbe permettere un controllo della personalità. Non sembra tuttavia che tale teoria colga nel segno, infatti il problema è sicuramente più pratico e la pericolosità dei dati ritraibili dalla scansione del volto e dalla sua fedele riproduzione potrebbe essere utilizzata per attribuire comportamenti non veri ai soggetti [59]. In questo senso gli strumenti di riconoscimento facciale permettono di violare il diritto ad una corretta e non infedele rappresentazione della propria identità che trova fondamento nell'art. 2 Cost. [60]. Un ulteriore pericolo è poi legato alla profilazione laddove la trasformazione delle sembianze umane in flussi di dati poi ricomposti e riconfigurati per confluire nel profilo assegnato, creano un sistema di forte spersonalizzazione e, nuovamente di assoluta mancanza di rispetto della complessa e complessiva personalità dell'individuo. Quest'ultimo, infatti, non può essere visto esclusivamente e isolatamente nella sua veste di consumatore, o utilizzatore di certe merci, o cliente finanziario con determinate caratteristiche, ma deve essere riguardato nel suo essere persona con specifici bisogni[61], poiché proprio nella necessità di distinguere tra identità e identificazione non sembra possibile accogliere l'opinione di quanti confondono l'identità digitale con gli strumenti di identificazione tecnologici o con le immagini, a volte usurpate, in ambito digitale[62], ma sembra necessario approdare ad una visione unitaria di identità personale che coinvolge anche comportamenti in ambito digitale.

6. Qualità del dato, pericolo di *bias* e valutazione d'impatto.

Da quanto riportato una linea comune definibile è la tematica della qualità del dato[63].

A ciò, tuttavia, sembra necessario aggiungere una riflessione sul problema delle correlazioni (a volte insospettabili) che l'algoritmo potrebbe individuare

---

[58] S. PORTER et al., *Is the Face a Window to the Soul? Investigation of the Accuracy of Intuitive Judgments of the Trustworthiness of Human Faces, in Canadian Journal of Behavioural Science*, 40, III, 2008, 171 ss.

[59] Il riferimento è alla nota tematica dei deepfake sulla quale v. M. CAZZANIGA, Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai *deepfakes*, in *Medialaws*, 2023, 170 - 187; Garante per la protezione dei dati personali, Deepfake*: Il falso che ti «ruba» la faccia (e la* privacy), scheda informativa sui rischi della manipolazione digitale di volti e voci, in www.garanteprivacy.it, 2020; A. SANTANGELO, *Il futuro del volto nell'era dei deep fake*, in AA.VV. *Il metavolto*, a cura di M. LEONE, FACETS Digital Press, 2022, 19 ss.; D. HARRIS, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, in *Duke Law & Technology Review*, 17, 2019, 99 ss.; V. AZZALI, N. ELLECOSTA, *La questione* deepfake *in Italia: una panoramica*, in *Medialaw*, 2023, 72 - 90.

[60] Così, non da ora, Cass., sez. I, 22.06.1985, n. 3769.

[61] P. PERLINGIERI, La personalità umana nell'ordinamento giuridico, Napoli, 1972.

[62] Discorre di possibile traslazione tra dato e persona, nelle ipotesi di utilizzo di dati biometrici S. EL SABI, *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, cit., 789 - 827.

[63] Su questo tema sembra molto opportuna la precisazione della Legge argentina n. 25.326, dove si prevede uno specifico articolo (il n. 4) sulla qualità del dato. Il tema è affrontato da numerosa dottrina. Cfr., E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leggi civ. comm.*, 2018, V, 1209-1236; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016, 254 ss.; G. FINOCCHIARO, Intelligenza Artificiale e protezione dei dati personali, in Giur. it., 2019, VII, 1670 - 1677.

ed implementare. Per dirlo in una parola è il pericolo di *bias*[64]. Per cui se, ad esempio, un database di volti è collegato a statistiche che individuano in una certa etnia una maggiore possibilità di commettere crimini, allora la discriminazione è quasi inevitabile.

La soluzione, come oramai da un po' ci ha abituato il legislatore europeo, è l'*accountability*, ossia la responsabilizzazione dell'operatore professionista[65] che sarà quindi anche chiamato ad una valutazione di impatto per i sistemi ad alto rischio.

Tanto è previsto nell'AI Act che specifica che tale procedimento deve valutare l'impatto di quei comportamenti sui diritti fondamentali [66] specificando anche gli elementi di tale valutazione, tra cui anche le categorie di persone fisiche e gruppi verosimilmente interessati, i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati e le misure da adottare qualora tali rischi si concretizzino.

Sembra, tuttavia, che tale Valutazione di impatto sia diversa da quella prevista dall'art. 35 del GDPR che è invece relativa all'impatto dei trattamenti previsti sulla protezione dei dati personali, mentre la tutela dei diritti e delle libertà delle persone fisiche vengono presi in considerazione solo con riferimento al rischio presunto.

Quanto questa differenza terminologica, che ora si nota, sia poi traducibile in una differenza di contenuto e di responsabilità è ancora troppo presto per dirlo, certo è che gli elementi individuati dal GDPR al comma 7 dell'art. 35 sono ben diversi da quello desumibili dall'art. 27 dell'AI ACT.

Di sicuro è che l'utilizzo di dati biometrici potrebbe colorare diversamente la rischiosità per i diritti fondamentali.

L'importanza della valutazione d'impatto è stata rimarcata di recente in un parere emesso dal Comitato europeo per la protezione dei dati a seguito di una richiesta dell'Autorità di vigilanza francese sull'uso della tecnologia di riconoscimento facciale da parte degli operatori aeroportuali e delle compagnie aeree per l'autenticazione o l'identificazione biometrica dei passeggeri per semplificare il flusso di passeggeri negli aeroporti[67].

Come osservazione preliminare, il Comitato ricorda che l'uso dei dati biometrici e in particolare della tecnologia di riconoscimento facciale comporta rischi maggiori per i diritti e le libertà degli interessati [68] . Dunque, si

---

[64] Sul punto cfr., A. PIN, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, cit., 3081 ss.; F. FAINI, *Big data, algoritmi e diritto*, in DPCE online, 2019, Vol. 40, III, 1869 ss.

[65] Tale responsabilizzazione porta anche ad imporre un costante controllo ed aggiornamento dei dati per non creare la situazione per cui continuino a perpetrarsi discriminazioni passate. Sul punto v., D. CARDON, *Che cosa sognano gli algoritmi.* Le nostre vite al tempo dei big data, Milano, 2016, 74.

[66] c.d. *fundamental rights impact assessment,* art. 27, AI ACT.

[67] Comitato europeo per la protezione dei dati, *Opinion on the use of facial recognition to streamline airport passengers' flow* (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, n. 11, 2024, Version 1.1. Adopted on 23 May 2024.

[68] I rischi significativi evidenziati sono soprattutto relativi alla intermediazione della macchina. Infatti, un sistema di riconoscimento facciale rende le caratteristiche intrinseche del soggetto "leggibili dalle macchine," creando un collegamento permanente tra corpo e identità. Questo trattamento può amplificare le minacce alla privacy e alla sicurezza personale, specialmente in caso di violazioni o accessi non autorizzati. La maggiore pericolosità di un eventuale trattamento automatizzato di questi dati sta nel fatto che in ipotesi di *data breach*, i dati biometrici non possono essere "cambiati" come una *password*, quindi le persone colpite sono permanentemente esposte a questo tipo di rischio. Inoltre, il documento sottolinea anche che le tecnologie di riconoscimento facciale possono essere soggette a *bias* legati a età, genere e razza. Questi pregiudizi algoritmici possono portare a trattamenti ingiusti e discriminatori, specialmente contro

raccomanda, che prima di utilizzare tali tecnologie, i titolari del trattamento valutino l'impatto del trattamento in linea con i requisiti dell'art. 35 GDPR e considerino se esistono mezzi meno invasivi che possano raggiungere lo scopo legittimo del trattamento.

Il parere è poi molto articolato e valuta quattro possibili scenari che sono contraddistinti da un grado crescente di automazione. In tutte le ipotesi si conclude che si potrebbe ritenere che le misure scelte abbiano soddisfatto il principio di necessità se il titolare del trattamento può dimostrare che non esistono soluzioni alternative meno invasive che potrebbero raggiungere lo stesso obiettivo in modo altrettanto efficace[69].

Ovviamente, in questo caso, il riferimento era alla valutazione di impatto di cui al GDPR ed è puro esercizio di stile chiedersi cosa avrebbe detto l'EDPB se fosse stato in vigore l'AI ACT.

Ma più che interrogarci su questo, sembra opportuno riflettere sulla ragionevolezza dell'applicazione delle norme nel caso concreto e richiamare fortemente il ruolo di un interprete consapevole e coraggioso che superi la contrapposizione tra privacy e persona, in una corretta interpretazione della normativa sul trattamento dei dati personali per approdare finalmente a quella evoluzione dal diritto ad essere lasciati soli al diritto al controllo della circolazione dei dati. In questo senso assume un ruolo centrale il c.d. diritto all'autodeterminazione informativa ricavabile dell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea che rappresenta il fondamento e il coordinamento delle normative di cui stiamo discutendo.

---

minoranze e gruppi vulnerabili, creando disuguaglianze nel modo in cui le persone sono identificate e trattate.

[69] Analogamente si è espresso il Garante italiano per la protezione dei dati personali, negando per ben 5 volte l'utilizzo di strumenti di riconoscimento facciale per il controllo della presenza dei lavoratori. Il Garante ha specificato che alla luce dei principi di minimizzazione e proporzionalità del trattamento, i datori di lavoro avrebbero dovuto optare per sistemi meno invasivi e rispettosi della sfera personale dei lavoratori. Si tratta dei seguenti provvedimenti: Provvedimento 22.02.2024, doc. web. n. 9995680. Ordinanza ingiunzione nei confronti di L'Igiene Urbana Evolution s.r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995785; Provvedimento 22.02.2024, doc. web. n. 9995701, Ordinanza ingiunzione nei confronti di Airone società consortile a r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995701; Provvedimento 22.02.2024, doc. web. n. 9995741, Ordinanza ingiunzione nei confronti di Blue Work s.r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995741; Provvedimento 22.02.2024, doc. web. n. 9995762, Ordinanza ingiunzione nei confronti di DM Technology s.r.l., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995762; Provvedimento 22.02.2024, doc. web. n. 9995785, Ordinanza ingiunzione nei confronti di Unica s.r.l.s., disponibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995785.

Carbajo Cascón F, 'Plataformas digitales y derechos de la personalidad' (2024) 2 EJPLT, 54 – 83.
DOI: https://doi.org/10.57230/EJPLT242FCC

EJPLT
ISSN 2704-8012



Plataformas digitales y derechos de la personalidad

Digital platforms and personality rights

FERNANDO CARBAJO CASCÓN
Catedrático de Derecho Mercantil
Universidad de Salamanca

Abstract

Algunos tipos de plataformas digitales, como las redes sociales, facilitan el encuentro e intercambio de opiniones, informaciones y contenidos entre usuarios que, con frecuencia, pueden vulnerar derechos de la personalidad de terceros, afectando a su privacidad. En su condición de intermediarios en línea las plataformas se benefician en la UE de un régimen de exención de responsabilidad frente a los daños que a terceros pueden causar las actividades, informaciones o contenidos compartidos por los usuarios de su servicio, siempre que se den ciertos y cumplan con los deberes de diligencia debida establecidos en el Reglamento de Servicios Digitales de 2022. De no cumplirse esas condiciones podrán resultar responsables de vulneraciones a los derechos de la personalidad o datos personales de terceros cometidas por los usuarios de su servicio de plataforma.

Some types of digital platforms, such as social networks, facilitate the meeting and exchange of opinions, information and content between users, which can often infringe the personality rights of third parties, affecting their privacy. As online intermediaries, platforms benefit in the EU from a regime of exemption from liability for damage that may be caused to third parties by activities, information or content shared by users of their service, provided that the due diligence duties set out in the Digital Services Regulation 2022 are met and complied with. Failure to comply with these conditions may make them liable for infringements of the personal rights or personal data of third parties committed by users of their platform service.

© The author(s) 2024, 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: Plataformas digitaes; Privacidad; Derechos de la personalidad; Datos personales; Responsabilidad de intermediarios en línea; Puerto seguro

Summary: 1. Planteamiento del problema. – 2. Concepto y tipos de servicios en línea. – 3. Régimen de responsabilidad de los servicios de plataforma en línea. – 3.1. Los precedentes: el régimen de puerto seguro establecido en la Directiva 2000/31/CE, de comercio electrónico. – 3.2. La interpretación del requisito del conocimiento efectivo por el Tribunal Supremo español. – 3.3. La interpretación del Tribunal de Justicia de la UE sobre el alcance de las reglas de puerto seguro. – 3.4. Ponderación de derechos e intereses por parte del intermediario en línea a la hora de cumplir con su deber de reacción diligente en la retirada de contenidos infractores de derechos de la personalidad de terceros. – 4. El régimen de responsabilidad de los intermediarios en línea en el reglamento de servicios digitales de la unión europea. – 4.1. Las reglas de exención de responsabilidad de intermediarios de alojamiento de datos en el Reglamento (UE) de Servicios Digitales. – 4.2. Obligaciones de diligencia debida de los prestadores de servicios de alojamiento de datos, en particular plataformas en línea de comercio electrónico. – 5. Naturaleza de la responsabilidad de los intermediarios en línea. En particular, su posible responsabilidad por intromisiones en la privacidad. – 5.1. Consideraciones previas sobre la clase de responsabilidad imputable a las plataformas digitales. – 5.2. La responsabilidad aplicable a las plataformas digitales en casos de intromisiones en la privacidad.

1. Planteamiento del problema.[1]

Internet permite a millones de usuarios acceder a todo tipo de contenidos, interactuar entre sí y generar contenidos propios o información en general ("*user-generated contents*") que comparten con el resto de internautas a través de diferentes tipos de aplicaciones y servicios en línea; desde páginas web, blogs o diarios y revistas digitales que generan y ofrecen información dejando espacio para los comentarios de los usuarios en foros de opinión, a grupos de chats (Whatsapp, Telegram) y redes sociales de distinta naturaleza (Facebook/Meta, Twitter/X, Instagram), pasando por servicios que agregan información generada por los usuarios (webs de enlaces) o que permiten compartir vídeos u otros contenidos (YouTube, Twitch, TikTok).

Estos servicios en línea han transformado radicalmente la forma en que las personas obtienen, suministran y comparten contenidos e información, opinan, comentan e interactúan entre sí, hasta el punto de crear y consolidar un nuevo contexto social y económico que identificamos como Sociedad de la Información, Sociedad Conectada o Sociedad Digital. La Red ofrece grandes oportunidades de negocio, consumo e interacción social, pero genera también

[1] El autor es Investigador Principal 1 del Proyecto de Investigación que lleva por título "Marco regulador de las plataformas en línea en la economía digital: competencia y responsabilidad en el uso de datos y contenidos (PID2020-119002RB-I00), financiado por el Ministerio de Ciencia e Innovación en el marco de los programas estatales de generación de conocimiento y fortalecimiento científico y tecnológico del sistema de i+d+i y de i+d+i orientada a los retos de la sociedad, para el periodo 1 de septiembre de 2021 a 31 de agosto de 2024.

grandes riesgos al constituir un cauce para realizar actividades ilícitas y comentarios lesivos de derechos de diferente naturaleza: derechos de marca, derechos de autor y derechos conexos, derechos sobre los datos personales o derechos de la personalidad (intimidad, honor y propia imagen), entre otros.

Internet ha supuesto así un paso de gigante para la democratización de la información, maximizando las libertades de expresión e información, al permitir a los usuarios acceder con facilidad a información plural, generar información por sí mismos y compartirla expresando sus opiniones libremente. Tan libremente -y sin pudor alguno en muchas ocasiones- que se ha convertido en un fenómeno habitual la utilización ilegítima de datos personales e imágenes para el insulto o la difamación a personas públicas (políticos, periodistas, deportistas, artistas, etc.) y privadas, atentando contra su honor, intimidad o imagen.

En este contexto debe analizarse cuidadosamente la posición que ocupan los servicios en línea cuando sus responsables y/o sus usuarios vulneran derechos de terceros en los contenidos e informaciones que generan y comparten entre sí; especialmente la posición de aquellos servicios en línea mixtos o híbridos que además de generar sus propios contenidos actúan como intermediarios en línea al permitir a los usuarios mostrar sus pareceres y comentarios en foros de opinión (diarios y revistas digitales), así como la de los servicios de intermediación puros que permiten a los usuarios interactuar entre sí compartiendo información y contenidos de muy diferente naturaleza (agregadores de información, redes sociales y servicios de compartición en línea).

Es claro que los servicios en línea que proveen y suministran contenidos o cualquier tipo de información generada por ellos mismos serán responsables -por hecho propio o por hecho ajeno, *ex* artículos 1902 y 1903 CC- de las posibles infracciones de derechos de terceros que puedan producirse con motivo de su actividad; entre ellas las intromisiones ilegítimas en la intimidad, el honor o a la propia imagen (cfr. artículo 18 CE y LO 1/1982, de 5 de mayo) o la utilización no autorizada de datos personales. Igualmente serán responsables directos por infringir derechos de terceros los usuarios (internautas) que generen o compartan contenidos ilícitos o que realicen comentarios atentatorios contra los derechos de la personalidad en cualquier servicio en línea del que sean titulares o usuarios, siempre que se les pueda identificar adecuadamente.

Pero cuando esos contenidos o informaciones son generados o compartidos por usuarios que recurren a servicios de intermediación en línea híbridos o puros para suministrarlos o compartirlos surgen dificultades inherentes a las propias características de la Red: la dificultad para identificar a usuarios que permanecen en el anonimato o que se esconden tras un alias o "*nick-name*" y la naturaleza de intermediarios de los servicios en línea que permiten a los usuarios compartir información. En estas situaciones es cuando se plantea la posición que deben ocupar los intermediarios en línea que facilitan a los usuarios el servicio técnico para llevar a cabo el intercambio de contenidos y de información que vulnera derechos de terceros: ¿Han de quedar exentos de toda responsabilidad por contenidos o informaciones generadas y compartidas por usuarios sobre los que no tienen ningún tipo de control?¿O se les puede considerar responsables por las infracciones de derechos de terceros realizadas

por los usuarios de su servicio si no despliegan una diligencia mínima para identificar y retirar los contenidos o informaciones infractores?

El anonimato es uno de los pilares de Internet y uno de los grandes atractivos para los usuarios a la hora de generar contenidos y expresar sus opiniones y comentarios; y está amparado legalmente en la medida en que los operadores de redes de comunicaciones y los proveedores de servicios en línea únicamente estarían obligados a revelar la identidad de los usuarios de sus servicios cuando medie un requerimiento judicial y solamente en casos de detección, investigación y enjuiciamiento de delitos graves (cfr. Ley 25/2007, de 18 de octubre, de conservación de los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que incorpora la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006), toda vez que los datos de las comunicaciones electrónicas se consideran datos de carácter personal que permiten extraer conclusiones sobre la vida de las personas[2]/[3].

Ante esta perspectiva los perjudicados por el suministro de contenidos ilegales o por comentarios o informaciones difamatorios tienen que dirigirse contra los servicios en línea que permiten visibilizar y compartir esos contenidos e informaciones generados por los usuarios de esos servicios que atentan contra sus derechos, bien para solicitar la retirada de esos contenidos o comentarios o bien para exigir responsabilidad por los daños y perjuicios sufridos si los intermediarios no realizan una actuación diligente para retirarlos. Incluso pueden preferir dirigirse contra los servicios en línea, aun cuando pudieran identificar a los usuarios responsables de los contenidos e informaciones infractores de sus derechos[4], por simples razones de economía procesal (la imposibilidad o poca eficacia práctica de dirigirse contra múltiples infractores y las dudas sobre su solvencia)[5].

---

[2] STJUE (Gran Sala), de 21 de diciembre de 2016 (Asuntos acumulados C-203/15 y C-698/15, "Tele2 Sverige y Watson y otros", ap. 99); y STJUE (Gran Sala) de 8 de abril de 2014 (Asuntos acumulados C-293/12 y C-594/12, "Digital Rights Ireland y Seitlinger y otros", ap. 27).

[3] Aunque el TJUE consideró nula la Directiva 2006/24/CE al considerar que la Directiva e-Privacy, y en especial su artículo 15, se opone (como norma general) a medidas legislativas que establezcan, para la prevención, la investigación, el descubrimiento y la persecución de delitos, la conservación generalizada e indiferenciada, con carácter preventivo, de los datos de comunicaciones electrónicas, admitiendo no obstante que las legislaciones nacionales promulgadas para incorporar esa Directiva pueden resultar válidas y eficaces siempre que cumplan el requisito de proporcionalidad, estableciendo reglas claras y precisas sobre el alcance de la conservación de datos y comunicaciones e impongan unas exigencias mínimas en relación con las circunstancias y requisitos que debe cumplir una medida para el tratamiento de datos personales. Sin embargo, el Tribunal Supremo español ha afirmado la plena vigencia y aplicación de la Ley 25/2007, de 18 de octubre, poniendo de manifiesto que recoge la exigencia de autorización judicial previa (artículo 6.1) para acceder a datos personales conservados por los operadores de redes de comunicaciones que no se contemplaba en la Directiva. Vid. POLO ROCA, A., "La regulación sobre la conservación de datos en las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión", IDP-Revista de Internet, Derecho y Política, nº 33, octubre de 2021, accesible en https//:idp.uoc.edu.

[4] El Tribunal de Justicia de la UE considera que la Directiva 2006/24 no excluye una normativa nacional como la basada en el artículo 8 de la Directiva 2004/48 del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, que, a efectos de la identificación de un abonado a Internet o de un usuario de Internet, permite que se requiera judicialmente a un proveedor de acceso a Internet para que comunique al titular de un derecho de autor la identidad del abonado a quien se ha asignado una determinada dirección IP que supuestamente ha servido para la vulneración de dicho derecho, al ser una materia ajena al ámbito de aplicación "*ratione materiae*" de la Directiva 2006/24. Cfr. STJUE de 19 de abril de 2012 (Asunto C-461/10, "Bonnier Audio").

[5] Vid. JULIÀ BARCELÓ, R., "Liability for Online-Intermediaries: A European Perspective", EIPR, 1998/12, p. 454.

Surgen importantes dudas, en particular, sobre la posición que tienen los servicios de intermediación en línea, especialmente aquellos que prestan servicios de alojamiento de datos ("*hosting*") o servicios de búsqueda y enlace ("*searching & linking*") al facilitar a los usuarios compartir contenidos e informaciones de distinta naturaleza, incluyendo datos e informaciones de carácter personal de terceros, ante posibles requerimientos y demandas de quienes resultan afectados por el uso indebido de datos personales o por intromisiones en su intimidad, su honor o su propia imagen[6].

2. Concepto y tipos de servicios en línea.

La legislación española (Anexo de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico; LSSICE), que trae razón de la legislación comunitaria europea (Directiva 2000/31/CE, de 8 de junio, del Parlamento Europeo y del Consejo, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior; DCE) ofrece un concepto claro de servicios de la sociedad de la información y de los servicios de intermediación: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, comprendiendo también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios[7]/[8].

Los servicios de intermediación se configuran como una especie dentro del género de los servicios de la sociedad de la información, definiéndolos el mentado Anexo LSSICE 2002 como aquellos servicios de la sociedad de la información por los que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información. De modo que un servicio de intermediación se convierte en pieza clave para utilizar cualesquiera otros servicios de la sociedad de la información. Se incluyen entre ellos los servicios de acceso a Internet ("*Internet Service Providers*"), los servicios de transmisión de datos por redes de telecomunicaciones ("*mere conduit*" o

[6] Vid. VAN DER SLOOT, B., "Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations en Europe", JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, accesible en https://www.jipitec.eu/issues/jipitec-6-3-2015/4318. Vid. también, LÓPEZ RICHARD, J., "Difamación en la Web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", Derecho Privado y Constitución, nº 26, enero-diciembre 2012, pp. 143-201 (cfr. pp. 147-148).

[7] La misma definición, con mayores explicaciones, se contiene en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo: Todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios; entendiendo por servicio "a distancia" un servicio prestado sin que las partes estén presentes simultáneamente, "por vía electrónica" un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético, y "a petición individual de un destinatario de servicios" un servicio prestado mediante transmisión de datos a petición individual (cfr. artículo 1.1 letra b.).

[8] Entre ellos se incluyen los servicios de contratación de bienes o servicios por vía electrónica (servicios de comercio electrónico); la organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales; la gestión de compras en la red por grupos de personas; el envío de comunicaciones comerciales; los servicios de suministro de información por vía telemática; el vídeo bajo demanda, como servicio en que el usuario pueda seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

"*routing*"), los servicios que ofrecen la realización de copia temporal de las páginas de Internet solicitadas por los usuarios ("*system caching*" o memoria tampón), los servicios de alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por terceros ("*hosting*") y los servicios que ofrecen instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet ("*searching & linking*").

Dentro de los servicios de intermediación en línea, los llamados "*Servicios de Plataforma*" son servicios de alojamiento o almacenamiento de datos (servicios de "*hosting*" 2.0). Estos intermediarios en línea responsables de los servicios de plataforma se han convertido en actores fundamentales del mercado y de la sociedad digitales, actuando en ocasiones como auténticos prestadores de servicios de intermediación en línea y en otras como generadores de sus propios contenidos o distribuidores de sus propias mercancías o servicios (plataformas híbridas o mixtas).

En esta línea, como una evolución del concepto básico de servicios de intermediación en línea, en el nuevo Reglamento (UE) 2022/2065, del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales, RSD, de aplicación a partir del 17 de febrero de 2024), se contemplan de forma específica las "plataformas en línea" como una subespecie de los servicios intermediarios del tipo o modalidad "*hosting*", definiéndolas en su artículo 3 letra i) como prestadores de servicios de alojamiento de datos que, a petición de un destinatario del servicio, almacenan y difunden al público información, salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento.

De forma similar, el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales; RMD) [9], establece en su artículo 2.2 que el "servicio básico de plataforma" hace referencia a cualquiera de los siguientes elementos: *a)* servicios de intermediación en línea; *b)* motores de búsqueda en línea; *c)* servicios de redes sociales en línea; *d)* servicios de plataformas de intercambio de vídeos; *e)* servicios de comunicaciones interpersonales independientes de numeración; *f)*

[9] En los mercados digitales los efectos de red directos e indirectos propios de los "*multi-side-markets*" creados en torno a las plataformas digitales (que sirven como punto de encuentro entre usuarios, entre éstos y los anunciantes, y entre oferentes y demandantes de productos y servicios), generan un efecto conocido como "*winner takes it all*" ("el ganador se lleva la mayoría") que favorece la adquisición de un importante poder de mercado por parte de algunas de estas plataformas hasta convertirlas en auténticos guardianes de acceso al mercado digital ("*Gatekeepers*"), circunstancia que ha forzado una regulación "*ex ante*" para frenar el excesivo poder de mercado de estas plataformas y garantizar así la equidad y disputabilidad de los mercados, por medio del nuevo Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). Vid. RUIZ PERIS, J.I. (Dir.), *Competencia, compensación de daños y mercados digitales*, Tirant lo Blanch, Valencia, 2022.

sistemas operativos; *g)* navegadores web; *h)* asistentes virtuales; *i)* servicios de computación en la nube; *j)* servicios de publicidad, incluidas las redes de publicidad, los intercambios publicitarios y cualquier otro sistema de intermediación publicitaria, prestados por una empresa que preste cualquiera de los servicios básicos de plataforma enumerados en las letras a) a i). Servicios de plataforma que tendrán la consideración de guardianes de acceso si cumplen con los requisitos o condiciones establecidos al efecto en el artículo 3 RMD.

En el presente estudio nos centraremos en la actividad de las plataformas digitales que ofrecen con carácter principal o accesorio un servicio de intermediación puro o mixto que facilita el intercambio de contenidos o todo tipo de opiniones e informaciones entre los usuarios de su servicio, incluyendo -en particular- los servicios de redes sociales.

3. Régimen de responsabilidad de los servicios de plataforma en línea.

Para poder abordar con claridad y garantías el régimen de responsabilidad de las plataformas digitales por posibles infracciones a la intimidad, el honor y la propia imagen de terceros, es preciso hacer un rápido recorrido por la normativa relativa a la responsabilidad o no responsabilidad de los servicios de intermediación en la sociedad de la información. Esto es, por el régimen general de exención de responsabilidad de los intermediarios en línea o normas de puerto seguro ("*safe harbour*"), tal y como fue regulada en la Directiva 2000/31 de Comercio Electrónico (DCE) y en la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE) e interpretada por el Tribunal Supremo y el Tribunal de Justicia de la Unión Europea.

La regla general es que los prestadores de servicios de la sociedad de la información, incluidos los servicios de intermediación en línea, están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de las reglas especiales de exención de responsabilidad previstas para los intermediarios en línea (cfr. artículo 13 LSSICE).

3.1. Los precedentes: el régimen de puerto seguro establecido en la Directiva 2000/31/CE, de comercio electrónico.

El artículo 14 de la Directiva 2000/31/CE, sobre servicios de la sociedad de la información, en particular el comercio electrónico ("Alojamiento de datos"), norma incorporada en el artículo 16 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico ("Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos"), establece las bases del beneficio de la exención de responsabilidad o puerto seguro para los servicios de intermediación consistentes en el almacenamiento de datos, disponiendo que el prestador de servicios no puede ser considerado responsable por los datos almacenados a petición de los destinatarios de su servicio a condición de que:

a) No tenga conocimiento efectivo de que la actividad o la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga

conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que;

b) En cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible;

c) La exención no se aplicará cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios.

El Considerando nº 42 de la Directiva 2000/31 aclara que las exenciones de responsabilidad establecidas en la presente Directiva sólo se aplican a aquellos casos en que la actividad del prestador de servicios de la sociedad de la información se limita al proceso técnico de explotar y facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros es transmitida o almacenada temporalmente, con el fin de hacer que la transmisión sea más eficiente. Esa actividad es de naturaleza meramente técnica, automática y pasiva, lo que implica que el prestador de servicios de la sociedad de la información no tenga conocimiento ni control de la información transmitida o almacenada. Este considerando actúa como pauta interpretativa del régimen de exención de responsabilidad de los intermediarios, y aunque inicialmente se previó aparentemente para los servicios de "*routing*" y "*caching*" de los proveedores de acceso a Internet (ISPs), el TS y el TJUE la extendieron más tarde a los servicios de "*hosting 2.0*" con los que se identifican los servicios de motores de búsqueda y las plataformas en línea de comercio electrónico.

El legislador español decidió ampliar el régimen de exención de responsabilidad a otra categoría de intermediarios: los prestadores de servicios de búsqueda y enlaces, disponiendo el artículo 17 LSSICE ("Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda") que este tipo de intermediarios no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

c) La exención de responsabilidad no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos

Es decir el legislador español establece un régimen de exención de responsabilidad común para los servicios de alojamiento de datos y de búsqueda y enlace, por más que los motores de búsqueda y los servicios que facilitan enlaces a otros sitios en línea actúan en realidad como servicios de alojamiento de datos "*lato sensu*"[10].

[10] Vid. CLEMENTE MEORO, M., "La responsabilidad civil de los prestadores de servicios de la sociedad de la información", en Clemente Meoro, M./Cavanillas Múgica, S. (Dirs.), *Responsabilidad civil y contratos en Internet. Su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Comares, Granada, 2003, pp. 1-116; APARICIO VAQUERO, J.P., "El nuevo régimen de prestación de servicios de la sociedad de la información", Revista de Derecho y Nuevas Tecnologías, 2003, núm. 2, pp. 87-111; PEGUERA POCH, M., *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Granada, 2007; y BUSTO LAGO, J.M., "La responsabilidad civil de los prestadores de servicios de la sociedad de la información

Ambas reglas se complementan con lo dispuesto en el artículo 15 de la misma Directiva 2000/31, que establece la inexistencia de una obligación general de supervisión para todos los servicios de intermediación ("*routing*", "*caching*" y "*hosting*"), disponiendo que los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar "*ex ante*" los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas. Esta regla general no impedirá, sin embargo, que un intermediario en línea pueda quedar sujeto a obligaciones de supervisión "*ex post*" ante reclamaciones dirigidas por terceros por contenidos o informaciones suministrados por los usuarios de su servicio.

El principal problema para delimitar la responsabilidad del intermediario de servicios de alojamiento reside en establecer qué debe entenderse por "conocimiento efectivo" de la ilicitud de los datos almacenados en su sistema. Conforme al tenor de la norma, no bastaría la mera sospecha de la actividad ilícita o un conocimiento abstracto de la posibilidad de que se estén lesionando bienes o derechos de terceros, sino que ha de ser un conocimiento actual, real o, como dice la Ley, "efectivo". Para intentar clarificar el alcance de este requisito, que se establece como regla básica para la exención de responsabilidad en ambos casos, el legislador español decidió ir más lejos de lo establecido en la DCE, indicando que se entenderá que el prestador de servicios de intermediación tiene el conocimiento efectivo de que determinada actividad o información incluida en su servicio por algún usuario es ilícita cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

Esta precisión sobre el alcance del requisito del conocimiento efectivo resultaba sumamente favorable para los prestadores de servicios de intermediación consistentes en el alojamiento de datos y de búsqueda de información y suministro de enlaces, ya que prácticamente les exime de todo tipo de diligencia en la identificación y retirada de información, contenidos o actividades compartida por los usuarios de su servicio que pueden vulnerar derechos de terceros salvo cuando tengan conocimiento por cualquier medio de que esa información, contenidos o actividades ha sido declarada ilícita por una resolución administrativa o sentencia judicial firmes.

No obstante, parece sugerirse que los servicios de intermediación tipo "*hosting*" y "*searching & linking*" pueden trabar conocimiento efectivo de posibles informaciones, contenidos o actividades ilícitos dentro de su plataforma o servicio de intermediación en línea si implementan procedimientos de detección y retirada ("*notice & take down*"). De modo que en el régimen de puerto seguro establecido en la DCE y LSSICE para los intermediarios de la sociedad de la información la implementación de estos servicios o procedimientos de denuncia y retirada tiene carácter meramente

(ISPs)", en Reglero Campos, L.F. (Dir.), *Tratado de Responsabilidad Civil*, T. II, Thomson-Aranzadi, Navarra, 2003, pp. 971 y ss., especialmente pp. 995 y ss.

voluntario, fruto de la autorregulación de los servicios de intermediación o con motivo de compromisos adquiridos en códigos de conducta generales o sectoriales. Con todo, su efectiva implementación lógicamente puede variar las condiciones establecidas sobre el alcance del conocimiento efectivo, pues se sugiere ("sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse") que si los intermediarios tuvieran conocimiento de actos, contenidos o informaciones ilícitas subidos y compartidos por los usuarios de servicio en línea a través de estos procedimientos técnicos de detección voluntariamente implementados estarían obligados a satisfacer el segundo requisito para exonerar su responsabilidad: reaccionar diligentemente para retirar esa información (incluyendo la retirada de enlaces) o impedir el acceso a la misma a los usuarios de su servicio, sin tener que esperar ya al conocimiento por cualquier medio de la existencia de una resolución administrativa o sentencia judicial firmes.

La Ley menciona que pueden establecerse "otros medios de conocimiento efectivo". Este último inciso actúa como cláusula de cierre de todo el sistema de responsabilidad, ya que pretende dar legitimidad a cualquier otra práctica que permita probar que el proveedor de alojamiento conocía (o debía conocer sin faltar a la buena fe) la ilicitud de los contenidos, actividades o informaciones que albergaban sus servidores. El supuesto paradigmático es la denuncia de la existencia de tales contenidos por parte de los afectados, aunque también puede considerarse el conocimiento público de la más que presunta ilicitud de determinadas informaciones alojadas en un determinado servidor (evidentes muchas veces en el caso de comentarios injuriosos, violaciones palmarias de la privacidad o ilícitos manifiestos contra derechos de autor y conexos o derechos de marcas y diseños industriales).

3.2. La interpretación del requisito del conocimiento efectivo por el Tribunal Supremo español.

La interpretación tan restrictiva del requisito del "conocimiento efectivo" realizada por el legislador español en los artículos 16 y 17 LSSICE, yendo más allá de lo previsto en la DCE, consagraba en la práctica un régimen de impunidad para los intermediarios de la sociedad de la información por las actividades o informaciones ilícitas de los usuarios de su servicio, con el consiguiente trastorno y -en algunos casos- indefensión para los titulares de derechos flagrante y masivamente vulnerados a través de esos servicios de agregación.

Sin embargo, esta interpretación tan restrictiva resultó corregida por la Sala Primera del Tribunal Supremo cuando en su Sentencia de 9 de diciembre de 2009 (caso "putasgae"), en un caso de infracción del derecho al honor de una persona jurídica, señaló que una interpretación tan restrictiva del "conocimiento efectivo" por parte del prestador de servicios de "*hosting*" no es conforme con la Directiva de Comercio Electrónico (cfr., Considerando nº 42 y artículo 14.1), "*ya que reduce injustificadamente las posibilidades de obtención del "conocimiento efectivo" de la ilicitud de los contenidos almacenados y amplía correlativamente el ámbito de la exención, en relación con los términos de la*

norma armonizadora, que exige un efectivo conocimiento, pero sin restringir los instrumentos aptos para alcanzarlo".

El TS realizó así una lectura del artículo 16.1 LSSICE (extensible al artículo 17 LSSICE) conforme al espíritu y finalidad de la DCE, la cual persigue un equilibrio adecuado entre la seguridad jurídica que necesitan los intermediarios de la sociedad de la información y el respeto a la libertad de expresión e información con la adecuada tutela de terceros que se puedan ver afectados por el uso que se haga de los servicios de esos intermediarios, permitiendo formas más flexibles de obtención del conocimiento efectivo de la ilicitud.

Concluyó entonces el Alto Tribunal ratificando la necesidad de una interpretación más flexible de las posibles formas de obtener el conocimiento efectivo por parte de los prestadores de servicios de alojamiento (y, por extensión, de los prestadores de servicios de enlaces a contenidos e instrumentos de búsqueda), apuntando al respecto que "*(A)demás de que el propio artículo 16 permite esa interpretación favorable a la Directiva -al dejar a salvo la posibilidad de "otros medios de conocimiento efectivo que pudieran establecerse"-, no cabe prescindir de que la misma atribuye igual valor que al "conocimiento efectivo" a aquel que se obtiene por el prestador del servicio a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate*".

Esta doctrina fue reiterada posteriormente por el Alto tribunal en casos similares de responsabilidad de intermediarios por actos de sus usuarios que suponen una intromisión en la intimidad, el honor o la propia imagen de terceros, en las SSTS (Civil) de 18 de mayo de 2010 (caso "quejasonline.com")[11], 10 de febrero de 2011 (caso "alasbarricadas.com", 26 de febrero de 2013 (caso "Ramoncín") y 5 de mayo de 2016 (caso "Izquierda Unida").

Por lo que se refiere al segundo requisito de exención de la responsabilidad de los intermediarios de la sociedad de la información, la STS de 18 de mayo de 2010 (caso "quejasonline.com") viene a reconocer que su valoración debe realizarse "*ad hoc*", a la luz de las circunstancias concurrentes en el caso concreto en torno a la mayor o menor diligencia del intermediario para, una vez detectada la información o actividad infractora, valorar la procedencia o improcedencia de su retirada o bloqueo de acceso. Es este precisamente el principal problema al que se deben enfrentar los intermediarios en línea cuando detecten por cualquier medio la existencia de actividades, contenidos o informaciones compartidos por los usuarios de su servicio que infringen derechos de terceros; muy particularmente en el caso de intromisiones ilegítimas en los derechos a la intimidad, al honor o la propia imagen: la decisión de si procede o no la retirada de ese contenido, actividad o información, pues ello exige que realicen una valoración de los distintos derechos en juego, por una parte los legítimos derechos de propiedad intelectual o derechos de la personalidad de los terceros afectados y por otra parte los también legítimos derechos a la libertad de expresión e información y de acceso a la información de los usuarios de su servicio de intermediación en línea.

[11] Vid. el comentario de RUBÍ PUIG, A., "Derecho al honor online y responsabilidad civil de ISPs", Indret.com, octubre 2010.

El problema de fondo reside en que la reacción diligente del intermediario para retirar actividades, contenidos o informaciones ilícitas de su plataforma en línea de las que tenga conocimiento por cualquier medio y evitar así cualquier tipo de responsabilidad por algo que realmente realizan los usuarios de su servicio, genera el riesgo de precipitación que puede desembocar en la vulneración de los derechos de sus usuarios y, con ello, de posibles demandas por infracción de los derechos constitucionales a la libertad de expresión e información o el legítimo acceso a la información (cfr. artículos 18 y 44 CE), así como de las propias reglas del contrato de prestación del servicio.

El Tribunal Supremo ha ratificado su doctrina sobre la interpretación más flexible del requisito del conocimiento efectivo en la STS 235/2020, de 2 de junio (caso "meneame.com"), relativo a infracción del derecho al honor en comentarios que contienen expresiones insultantes a partir de una información subida por un usuario (en forma de enlace) sobre un determinado cargo político. Considera el Alto Tribunal que el servicio de intermediación (web de enlaces de prensa compartidos por los usuarios) tuvo conocimiento efectivo de las expresiones injuriosas incluidas en un foro de opiniones a partir de la denuncia efectuada por el afectado a través de un correo ordinario y un burofax, sin que hubiera una reacción diligente del intermediario para retirar esa información o bloquear su acceso desde la plataforma.

En respuesta al recurso de amparo formulado por el responsable del servicio de intermediación planteando un conflicto entre la protección del derecho al honor y la libertad de expresión e información, el Tribunal Constitucional responde en su STC 83/2023, de 4 de julio (caso "meneame.com") que el requisito del conocimiento efectivo puede y debe interpretarse en sentido amplio (pudiendo obtenerse a través de cualquier método idóneo) para conjugar adecuadamente los distintos intereses y derechos involucrados, concluyendo que no se produce una lesión del derecho a la tutela judicial efectiva (artículo 24 CE) ni a la libertad de expresión e información (artículo 20 CE) por el hecho de interpretar en sentido amplio dicho requisito del conocimiento efectivo.

3.3. La interpretación del Tribunal de Justicia de la UE sobre el alcance de las reglas de puerto seguro.

Primero en la STJUE (Gran Sala) de 23 de marzo de 2010 (Asuntos acumulados C-236/08 a C-238/08, "Google France"), y más tarde en la STJUE (Gran Sala) de 12 de julio de 2011 (Asunto C-324/09, "L'Oréal c. eBay Uk"), el Tribunal de Justicia de la UE puso las bases de la interpretación de las reglas de puerto seguro de los intermediarios de la sociedad de la información[12]. Aunque se trata de sentencias dictadas en materia de infracciones marcarias, dado el carácter horizontal del régimen de puertos seguros en materia de exención de responsabilidad de los intermediarios en línea, la doctrina del TJUE se puede

[12] Vid. DE MIGUEL ASENSIO, P.A., "Comercio electrónico y protección de marcas: Aspectos internacionales", en AA.VV., *Problemas actuales de derecho de la propiedad industrial (VIII Jornadas de Barcelona de Derecho de Propiedad Industrial)*, Tecnos, Madrid, 2018, pp. 17-63. Vid. también CARBAJO CASCÓN, F., "Las plataformas digitales ante la distribución de mercancías y el suministro de contenidos digitales ilícitos", Revista de Derecho de la Competencia y de la Distribución, nº 30, enero-junio 2022, pp. 7 y ss.

considerar aplicable a cualquier otro tipo de responsabilidad que pudiera imputarse a los usuarios de los servicios de intermediación de la modalidad de alojamiento de datos o "*hosting*", pues el Tribunal aclara de antemano que los motores de búsqueda fungen realmente como servicios de alojamiento de datos al proporcionar información mediante enlaces a sus usuarios.

Según el TJUE los prestadores de servicios de alojamiento de información no responderán por los actos de sus usuarios siempre que:

a) Actúen de forma neutral, automática y pasiva, y;

b) cuando tengan conocimiento por cualquier medio de una información o acto ilícito, reaccionen diligentemente para retirar la información ilícita o inhabilitar el acceso a la misma.

Expresado en sentido inverso, como excepción a la regla general que establece la exención de responsabilidad de los intermediarios en línea, los prestadores de servicios de alojamiento de información serán responsables de los actos cometidos por los usuarios de su servicio:

a) cuando no actúen de forma neutral, automática y pasiva, desempeñando un papel activo que les permita tener conocimiento, por cualquier medio, de los datos e informaciones ilícitos de sus usuarios y les presten asistencia para optimizar y promover la presentación y oferta de sus productos, servicios o contenidos, o;

b) cuando actuando de forma neutral, automática y pasiva tengan conocimiento efectivo por cualquier medio de infracciones a derechos de terceros cometidas por los usuarios de su servicio y no actúen con prontitud para retirar la información o imposibilitar el acceso a los mismos.

En definitiva, el TJUE deja claro que las reglas de puerto seguro sólo se aplicarán a los prestadores de servicios de alojamiento de información cuando actúen como intermediarios puros, siendo su actuación neutral, automática y pasiva en relación con las informaciones almacenadas por los usuarios de su servicio. Y establece asimismo el alcance del principio de reacción diligente en el caso de esas actuaciones como verdaderos intermediarios, señalando que la exención de responsabilidad sólo tendrá lugar si reaccionan con prontitud para retirar información ilícita de su plataforma cuando tengan conocimiento por cualquier medio de su existencia.

Para evitar interpretaciones excesivamente restrictivas de qué debe entenderse por "conocimiento efectivo", el Tribunal señala que para retirar el beneficio de la exención de responsabilidad bastará con que el intermediario haya tenido conocimiento "por cualquier medio" (incluidas reclamaciones de los titulares de derechos afectados en servicios de "*notice & take down*" implementados voluntariamente por la propia plataforma en línea) de hechos o circunstancias a partir de los cuales un operador económico diligente hubiera debido deducir ese carácter ilícito y actuar rápidamente para retirar los datos o impedir su acceso [13]. Así pues, para eludir el régimen de exoneración de responsabilidad de las plataformas digitales, será necesario acreditar que el intermediario conocía o al menos debería conocer sin faltar a la buena fe objetiva el carácter ilícito de las actividades o informaciones en cuya edición, promoción y difusión colabora y, a pesar de ello, no adoptó ninguna medida

[13] Cfr. STJUE de 12 de julio de 2011, Asunto "*eBay*", apartados 120 y 124.

para retirarlas de su plataforma. Pero no sólo eso, pues en la STJUE (Gran Sala) de 12 de julio de 2011 (Asunto C-324/09, "L'Oréal c. eBay Uk") el Tribunal aclara que la reacción diligente debería implicar no sólo la inmediata retirada de los datos o informaciones infractoras de derechos de terceros cuando el gestor del servicio de intermediación reciba un aviso o reclamación judicial o extrajudicial del titular de derechos afectado ("*notice & take down*"), sino también la adopción de medidas eficaces para evitar que esos datos o informaciones infractoras vuelvan a ser cargadas en la plataforma ("*notice & stay down*").

No siendo posible exigir una supervisión general "a priori" de la información que almacenan a los prestadores de servicios de alojamiento de datos, vedada por el artículo 15 de la Directiva 2000/31, se abre la puerta sin embargo a una supervisión particular "a posteriori" y "para casos específicos", cuando el intermediario tenga conocimiento por cualquier medio de la existencia de actos o informaciones que vulneran derechos de terceros; en particular, cuando reciban una comunicación o notificación motivada por parte de terceros afectados. El TJUE considera, en concreto, que es posible dirigir requerimientos efectivos y proporcionados a los operadores de mercados electrónicos para que, si éstos no deciden por sí mismos suspender la cuenta de quien vulneró los derechos de marca reclamados para evitar que el mismo usuario vuelva a cometer infracciones de esta naturaleza en relación con las mismas marcas, puedan ser obligados a ello mediante una orden judicial[14].

El propio TJUE ratificó esta postura en su STJUE de 3 de octubre de 2019 (Asunto C-18/18, "Eva Glawischnig Piesctek v. Facebook"), en relación con infracciones al derecho al honor y a la intimidad, donde dispuso que la Directiva 2000/31/CE no se opone a que un Tribunal pueda obligar a un prestador de servicios de alojamiento de datos (en el caso una red social) a suprimir los datos que almacene, y cuyo contenido sea idéntico al de una información declarada ilícita con anterioridad, o a bloquear el acceso a ellos, sea quien fuere el autor de la solicitud de almacenamiento de tales datos. De esta forma, cuando un servicio de plataforma (o, más en general, un servicio de intermediación tipo "*hosting*") no reaccione con prontitud para retirar información que vulnera derechos de terceros, a petición de los perjudicados u obligado por un tribunal, podría resultar responsable ante una demanda de esos terceros en reclamación de daños y perjuicios[15].

En particular esta relevante decisión del TJUE dispone que el artículo 15 DCE debe interpretarse en el sentido de que no se opone a que un tribunal de un Estado miembro pueda obligar a un prestador de servicios de alojamiento de datos a suprimir o bloquear: *i)* el acceso a datos o informaciones que almacene y cuyo contenido sea idéntico al de una información declarada ilícita con

---

[14] Cfr. STJUE de 12 de julio de 2011, Asunto "*eBay*", apartado 141. Del mismo modo, es posible requerir al operador para que adopte medidas que faciliten la identificación de sus clientes vendedores, pues si bien es cierto que resulta necesario respetar la protección de datos personales, no lo es menos que, cuando el autor de la infracción actúa en el tráfico comercial y no en el ámbito de su esfera privada, debe ser claramente identificable, de acuerdo con la filosofía del artículo 6 de la Directiva 2000/31/CE (cfr. apartado 142). Vid. SCHRIJVERS M., "European Court Rules on the Position of eBay Regarding the Sale of Infringing Products: L'Oreal v eBay", EIPR, Vol. 33, nº 11, 2011, pp. 723-724.

[15] Vid. un repaso a la jurisprudencia española en GONZÁLEZ SAN JUAN, J.L., "Jurisprudencia española sobre la protección del honor, la intimidad y la propia imagen en Internet", Ibersid, nº 9, 2015, pp. 83-88.

anterioridad; *ii)* siempre que la supervisión y la búsqueda de los datos a los que se refiera la medida cautelar judicial se limiten a aquellos que transmitan un mensaje cuyo contenido permanezca esencialmente inalterado con respecto al que dio lugar a la declaración de ilicitud y que contenga los elementos especificados en dicha medida, y en la medida en que las diferencias en la formulación de dicho contenido similar al que caracteriza a una información declarada ilícita con anterioridad no puedan obligar al prestador de servicios de alojamiento de datos a realizar una apreciación autónoma de ese contenido; iii) pudiendo extenderse esa obligación de supresión o bloqueo a nivel mundial en el marco del Derecho internacional pertinente.

Con ello se contempla la posibilidad de que un Juez o Tribunal de un Estado miembro imponga a un prestador de servicios de alojamiento mediante una medida cautelar la obligación de filtrar contenidos idénticos a los ya retirados tras haber sido declarados ilícitos, así como otros similares, siempre y cuando sea posible detectarlos mediante técnicas o medios de búsqueda y reconocimiento automatizado, y siempre y cuando no obliguen al prestador de servicios a realizar una valoración autónoma (no automatizada) del carácter infractor de esos contenidos o informaciones. Esto es, el TJUE viene a admitir que este filtrado específico "a posteriori" no constituye una labor de supervisión general (vedada por el artículo 15 DCE) ni tampoco supone una carga excesiva para el intermediario, siempre y cuando no obligue a una supervisión autónoma no automática de esos contenidos o informaciones.

3.4. Ponderación de derechos e intereses por parte del intermediario en línea a la hora de cumplir con su deber de reacción diligente en la retirada de contenidos infractores de derechos de la personalidad de terceros.

Para poder exonerar su responsabilidad ante posibles infracciones a la intimidad, el honor o la propia imagen resultante de contenidos, informaciones o comentarios suministrados o proferidos por los usuarios de su servicio, el intermediario en línea que tenga conocimiento de su existencia por cualquier medio (en particular si tuviera incorporados en su servicio mecanismos de denuncia o notificación y retirada o bloqueo) deberá realizar una ponderación de los intereses en juego, y, con ello, de derechos constitucionales frecuentemente confrontados, antes de proceder a la retirada o bloqueo de acceso a los mismos.

Los intermediarios en línea se sitúan, así, en una auténtica encrucijada, al tener que realizar una ponderación, compleja "*per se*", entre los derechos constitucionales al honor, la intimidad y la propia imagen de los terceros afectados (artículo 18 CE) y los derechos constitucionales a la libertad de expresión e información de los usuarios de su servicio (artículo 20 CE), a fin de eludir una posible responsabilidad indirecta por la infracción de tales derechos, viéndose obligados así a anticipar un juicio cuyo control último corresponde a los Tribunales de Justicia y, en último término, al Tribunal Constitucional.

Nace así un conflicto a tres bandas con motivo de la actividad de los intermediarios en línea, entre el denunciante titular de derechos presuntamente infringidos, el prestador del servicio de alojamiento y el usuario de su servicio que genera y/o comparte contenidos o informaciones

presuntamente atentatorios contra la privacidad, el honor o la imagen, el cual podría reclamar responsabilidades al intermediario si retirase información con motivo de una denuncia del titular de derechos que considerase absolutamente infundada o cuando menos dudosa[16]. El prestador de servicios de alojamiento se sitúa en el centro de esa encrucijada entre, de un lado, los derechos al honor, la intimidad y la propia imagen (u otros derechos como la propiedad industrial e intelectual), y de otro lado, los derechos a la libertad de expresión e información.

La sentencia del Tribunal Europeo de Derechos Humanos (ECtHR) de 10 de octubre de 2013 ("Delfi AS v. Estonia", 64569/09) y la posterior sentencia de la Gran Cámara de 16 de junio de 2015 ("Delfi AS v. Estonia", 64569/09) establecieron que un portal de noticias en línea que facilita a los usuarios reaccionar sin identificarse frente a las informaciones publicadas mediante un foro de comentarios tiene derecho a invocar la libertad de expresión pero debe también responder por los comentarios de los usuarios de su servicio que dañen intereses y derechos de terceros relacionados con la privacidad y el honor[17].

El Tribunal Europeo de Derechos Humanos entendió que, al publicar un artículo sobre la empresa de transporte marítimo, el portal de noticias Delfi tenía que haber previsto posibles reacciones negativas por parte del público y un riesgo mayor de que los comentarios excedieran de lo que puede considerarse una crítica aceptable para incurrir en auténticas injurias contra la empresa, razón por la que cabía esperar del portal de noticias mayores cautelas en la vigilancia y retirada de esos posibles comentarios injuriosos[18]. Aunque el portal tenía implementados procedimientos para detectar y retirar automáticamente comentarios excesivos (en forma de filtros de palabras inapropiadas y un sistema de notificación y retirada para los terceros afectados), consideró que su actuación como intermediario no fue lo suficientemente diligente para evitar causar daños al honor y reputación de terceros, sobre todo porque reaccionó muy tarde para retirar los comentarios injurioso, máxime cuando se benefició de la polémica con una mayor afluencia de usuarios que pueden realizar comentarios sin necesidad de identificación ni registro[19].

---

[16] El ordenamiento estadounidense, antes visto, otorga una garantía de no responsabilidad al proveedor de alojamiento siempre que en la retirada de contenidos se ajuste al estricto procedimiento previsto en la Sect. 512 c) 17 USC.

[17] En el caso, ante una denuncia de una empresa de transporte marítimo por los múltiples comentarios injuriosos vertidos por usuarios del portal de noticias estonio delfi.ee, este intermediario decidió retirar los comentarios pero no atendió la solicitud de indemnización. Los tribunales estonios decidieron que Delfi tenía que indemnizar a la empresa de transportes demandante. Elevada la cuestión a la Corte Europea de Derechos Humanos por infracción del artículo 10 del Convenio Europeo de Derechos Humanos (libertad de expresión), el Tribunal consideró que los tribunales estonios no habían interferido ilegítimamente en el derecho a la libertad de expresión al declarar al portal de noticias Delfi responsable de los comentarios publicados por los usuarios de su portal de noticias.

[18] Sobre la responsabilidad de intermediarios por infracciones al honor de personas jurídicas cometidas por los usuarios de su servicio, en particular analizando el asunto Delfi, véase GARCÍA SILVA, M., "La protección del derecho al honor de las personas jurídicas en redes sociales. La vía civil y la responsabilidad de las plataformas digitales", Aranzadi Civil, nº 8, septiembre 2022 (versión digital).

[19] Vid. VAN DER SLOOT, B., "Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations en Europe", cit., pp. 7-9.

En relación con el conflicto habitual entre derechos de la personalidad y la libertad de expresión e información, conviene recordar la doctrina del Tribunal Europeo de Derechos Humanos a la hora de ponderar el peso de ambos derechos fundamentales en una concreta situación. Señala en concreto que cuando se trata de contrastar el derecho a la libertad de expresión contra el derecho al respecto a la privacidad, el equilibrio o balance de intereses ha de tener en cuenta, entre otros, los siguientes elementos: la contribución de la información a un debate de interés general, el mayor o menor grado de conocimiento público de la persona natural o jurídica afectada por la información, el objeto del reportaje o información, la conducta previa de la persona afectada, el método de obtener la información y su veracidad, el contenido, forma y consecuencias de la publicación y la severidad mayor o menor de la sanción o indemnización solicitada[20].

De acuerdo con la doctrina del Tribunal Supremo y del Tribunal Constitucional[21], el juicio de ponderación constitucional entre libertad de expresión e información y los derechos de la personalidad requiere un examen de la intensidad y trascendencia con que cada derecho pueda resultar afectado en una situación determinada, respetando la posición prevalente inicial de las libertades de expresión e información teniendo en cuenta la mayor o menor relevancia o interés público de la información, por razón de la materia y/o de las personas, y la necesaria proporcionalidad en la difusión de las opiniones, debiendo proscribirse el empleo de expresiones manifiestamente injuriosas, vejatorias o que no guarden relación con la información o no sean necesarias para transmitir la idea crítica[22]. Cuando los afectados por informaciones y comentarios difundidos públicamente son personas de relevancia pública, ejercen funciones públicas o resultan implicados en asuntos de relevancia pública, el Tribunal Constitucional pone en primer plano un nivel máximo de eficacia justificadora del ejercicio de la libertad de expresión frente al derecho al honor que tendrá así una protección menor[23], del mismo modo que será inferior la tutela del derecho honor frente a la libertad de expresión e información cuando su titular sea una persona jurídica[24].

Pues bien, si el intermediario en línea (plataforma digital) realiza una valoración precipitada de este complejo conflicto, optando por retirar -sin una cuidadosa motivación- la información o contenidos presuntamente infractores de derechos de la personalidad de terceros, puede encontrarse con una demanda dirigida contra él por la infracción del derecho a la libertad de opinión, expresión e información del artículo 20 CE. Por el contrario, si decide conservar la información presuntamente infractora, puede encontrarse con una demanda de responsabilidad civil, *ex* artículo 1902 CC, interpuesta por el tercero

[20] Cfr. sentencias del Tribunal Europeo de Justicia (ECtHR) de 14 de junio de 2007 (Associes v. France, 71111/01) y de 12 de junio de 2012 (MGN Ltd/UK, 39401/04), entre otras.
[21] Cfr. STC 58/2018; STC 133/2018; SSTS 488/2017, de 11 de septiembre ó 429/2019, de 16 de julio.
[22] A diferencia de lo que sucede con la libertad de expresión, la libertad de información trata sobre la difusión de hechos objetivos, razón por lo que las opiniones y comentarios realizados por personas que no son profesionales de la información gozarán de mayor libertad (o menores restricciones) mientras que las informaciones expresadas por profesionales de los medios de comunicación están sujetos a los requisitos de diligencia y veracidad (cfr. STC 232/2002, de 9 de diciembre)
[23] Cfr. STC 344/2015, de 16 de junio.
[24] Cfr. STC 35/2017, de 19 de enero. Vid. GARCÍA SILVA, "La protección del derecho al honor de las personas jurídicas en redes sociales…", cit., pp. 4-5 (versión digital).

afectado por esa información, contenidos o comentarios, sobre todo cuando hubiera notificado por cualquier medio la existencia de la misma en la plataforma o servicio del intermediario y vio cómo éste no reaccionaba de forma diligente para retirar la información.

En ocasiones, las intromisiones en el honor, la intimidad o la propia imagen son tan evidentes ("*res ipsa loquitur*") que el intermediario no debería tener ninguna duda a la hora de reaccionar con prontitud para retirar la información o contenidos infractores de su plataforma o servicio de intermediación en línea[25]. Es el caso, por ejemplo, de los graves atentados a la intimidad, el honor y a la propia imagen que tienen lugar con las llamadas prácticas de "*deepfake*" o "ultrafalsificaciones"; sobre todo las "*porno deepfake*" consistentes en la utilización de imágenes de personas famosas para crear fotografías de desnudos o vídeos pornográficos falsos mediante programas de inteligencia artificial[26]. También en aquellos otros casos donde se manipula la voz a imagen de personas famosas para crear noticias falsas o en los que se usa la voz de intérpretes famosos -incluso ya fallecidos- cantando canciones creadas por inteligencia artificial[27].

Pero en otros casos donde la intromisión en derechos de la personalidad no resulte tan evidente el intermediario deberá realizar una cuidadosa y diligente ponderación, debidamente motivada, si quiere evitar demandas o reclamaciones por parte de los terceros afectados por la información, de un lado, o de los usuarios de su servicio, por otro lado[28].

En el caso de indebido tratamiento y difusión de datos personales (que constituye también un derecho de la personalidad o de la privacidad entendida "*lato sensu*", pero diferente del derecho a la intimidad, honor e imagen) en plataformas digitales, se estará a lo dispuesto en las propias políticas de algunas plataformas y en la normativa específica del sector[29], aplicándose las

[25] Cfr. STS 235/2020, de 2 de junio y STC 83/2023, de 4 de julio (caso "meneame.com").

[26] Son archiconocidos los casos que han afectado a las cantantes Rosalía y Taylor Swift (con más de 35 millones de visualizaciones en la red social X antes de que ésta procediera a eliminar esos contenidos de su plataforma). En nuestro país, sin afectar a personas famosas, resultó impactante el caso de las imágenes manipuladas presentando desnudas a un grupo de menores de Almendralejo.

[27] El incremento de casos de "*deepfakes*" llevó al Parlamento Europeo a encargar el estudio *Tackling Deepfakes in European Policy*, julio 2021 (algunas de cuyas conclusiones se han plasmado en el Reglamento UE sobre Inteligencia Artificial). En este estudio se ha inspirado seguramente el Grupo Parlamentario Sumar para promover un cambio legislativo por medio de la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, publicado en el Boletín Oficial de las Cortes Generales el día 13 de octubre de 2023, proponiendo cambios en la Ley 13/2022, de 13 de julio, General Audiovisual, en la LO 1/1892, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen, el Código Penal (para modificar el delito de injurias), la Ley de Enjuiciamiento Civil (para crear una medida cautelar específica), la LO 3/2018, de Protección de datos personales y garantía de derechos digitales, y la Ley 3/1991, de 5 de enero, de Competencia Desleal, entre otras.

[28] Vid. LÓPEZ RICHARD, J., "Difamación en la Web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", cit., pp. 143-201.

[29] El artículo 1.5 b) de la Directiva 2000/31, de comercio electrónico dispuso que la Directiva no se aplica a cuestiones relacionadas con la protección de datos personales en la sociedad de la información. El artículo 2.4 g) RSD 2022 señala que las reglas sobre responsabilidad de los intermediarios en línea previstas en el mismo se entenderán sin perjuicio del Derecho de la Unión en materia de datos personales. Por su parte, el artículo 2.4 del Reglamento (UE) 2016/678 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, dispone que su normativa se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

sanciones pertinentes directamente a las plataformas digitales en los casos en que la plataforma sea el responsable del tratamiento de los datos personales, e indirectamente, en su caso -aplicando las reglas de responsabilidad de intermediarios en línea,- cuando los responsables del tratamiento ilícito sean usuarios de la plataforma pero ésta no actúe como verdadero intermediario (neutral y pasivo) o, haciéndolo, cuando no reaccione con prontitud para la retirada de los mismos de su sitio en línea una vez advertida del tratamiento ilegítimo de datos personales por cualquier medio y en particular por la denuncia de los titulares de esos datos[30].

Estas complejas situaciones, cada vez más frecuentes debido al creciente protagonismo de las plataformas digitales en la sociedad digital como punto de encuentro y comunicación, venían reclamando reglas más precisas para delimitar el contenido del requisito de la reacción diligente de los intermediarios a la hora de retirar información, contenidos o comentarios infractores de derechos de terceros, y muy en particular de derechos de la personalidad, y ofrecer seguridad jurídica a todas la partes implicadas: los usuarios de servicios de intermediación en línea, los terceros afectados por los contenidos, informaciones o comentarios compartidos por esos usuarios y el gestor del servicio de intermediación en línea.

Estas reglas han sido desarrolladas por las instituciones de la Unión Europea en el nuevo Reglamento de Servicios Digitales aprobado por las instituciones de la Unión Europea y normativa ulterior de desarrollo del mismo.

4. El régimen de responsabilidad de los intermediarios en línea en el reglamento de servicios digitales de la unión europea.

4.1. Las reglas de exención de responsabilidad de intermediarios de alojamiento de datos en el Reglamento (UE) de Servicios Digitales.

El nuevo Reglamento (UE) 2022/2065, del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales; en adelante RSD), cuya plena aplicación tendrá lugar a partir del 17 de febrero de 2024[31], apuesta por la conservación de las reglas generales de exención de responsabilidad de los servicios de intermediación en línea establecidas en la Directiva 2000/31, de comercio electrónico (DCE), si bien considera conveniente precisar determinados elementos de ese marco normativo teniendo en cuenta la jurisprudencia del TJUE (Considerando nº 16).

Por lo tanto, el Reglamento de Servicios Digitales conserva el enfoque horizontal de las reglas de puerto seguro o exención de responsabilidad de los servicios intermediarios por los datos o informaciones transmitidos o almacenados a petición del usuario de sus servicios, señalando que sólo

[30] VAN DER SLOOT, B., "Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations en Europe", cit., pp. 5-6.

[31] El Reglamento de Servicios Digitales se aplica a las plataformas digitales y motores de búsqueda de muy gran tamaño que fueron designados por la Comisión Europea en una Decisión de 25 de abril de 2023 (DO C 249 de 14 de julio de 2023, p. 2), ejerciendo frente a ellos las competencias de ejecución previstas en el Capítulo IV, Secc. 4, artículo 49.3 del mismo RSD.

determinan cuándo no se pueden exigir responsabilidades al prestador de servicios intermediarios en relación con contenidos o informaciones ilícitos proporcionados por los destinatarios del servicio, sea cual sea la naturaleza del contenido ilícito y de la responsabilidad, correspondiendo así a las disposiciones de los ordenamientos nacionales determinar cuándo se pueden exigir responsabilidades a los prestadores de servicios intermediarios (Considerando nº 17 RSD).

En relación con los servicios intermediarios de alojamiento de datos, entre los que el propio Reglamento sitúa, como subespecie, a los servicios de plataforma en línea, el artículo 6, apartados 1 y 2 RSD reproduce la misma regla general de exención de responsabilidad que antes recogía el artículo 14 DCE, de modo que no serán responsables de las informaciones almacenadas por los destinatarios de su servicio a condición de que:

a) no tengan conocimiento efectivo de una actividad ilícita o de un contenido ilícito, o de hechos o circunstancias que revelen el carácter ilícito de una actividad o un contenido, o de que;

b) en cuanto tengan conocimiento de estas circunstancias actúe con prontitud para retirar el contenido ilícito o inhabilitar el acceso al mismo (el llamado principio de reacción diligente).

Lo anterior siempre que el usuario no actúe bajo la autoridad o el control del prestador de servicios, en cuyo caso se entiende que éste será en todo caso directamente responsable de los daños y perjuicios causados por la actividad o información suministrada por el usuario de su servicio[32].

Con todo, el artículo 6.3 RSD establece una nueva regla de responsabilidad directa de los intermediarios de alojamiento de datos y plataformas en línea en caso de infracciones de derechos de los consumidores y usuarios, en aquellos casos de plataformas de comercio electrónico que permitan celebrar contratos en línea entre usuarios profesionales y usuarios finales, cuando sean los intermediarios quienes presenten el elemento de información concreto o hagan posible la transacción comercial de manera que puedan inducir a un consumidor medio a creer que esa información o el producto o servicio objeto de la transacción se proporcione por la propia plataforma en línea por un usuario comercial que actúe bajo su control o dirección.

El artículo 8 RSD reproduce la inexistencia de una obligación general de supervisión "*ex ante*" de los intermediarios que establecía el artículo 15 DCE, al indicar que no se impondrá a los prestadores de servicios intermediarios ninguna obligación general de monitorizar la información que transmitan o

[32] El Considerando nº 18 RSD recoge la jurisprudencia del TJUE para ayudar a la interpretación de las normas de puerto seguro de los servicios intermediarios, pensando fundamentalmente en los servicios de alojamiento de datos o servicios de plataforma. Apunta, así, que las exenciones de responsabilidad establecidas en el Reglamento de Servicios Digitales para los prestadores de servicios de "*hosting*" no deberán aplicarse cuando, en lugar de limitarse a la prestación neutra de los servicios mediante un tratamiento puramente técnico y automático de la información proporcionada por el destinatario del servicio, el prestador de servicios intermediarios desempeñe un papel activo de tal índole que le confiera el conocimiento de dicha información, o control sobre ella. En la misma línea, el Considerando nº 20 RSD apunta que cuando un prestador de servicios intermediarios colabore deliberadamente con un destinatario de los servicios a fin de llevar a cabo actividades ilícitas, se ha de considerar que el servicio no se ha prestado de forma neutra y, por tanto, no debe poder acogerse a las exenciones de responsabilidad estipuladas en el Reglamento. Y en el Considerando nº 23 se indica, en concreto, que la exención de responsabilidad no puede aplicarse cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios de alojamiento.

almacenen, ni de buscar activamente hechos o circunstancias que indiquen la existencia de actividades ilícitas; aunque el artículo 7 RSD deja abierta la posibilidad de que los intermediarios realicen, de buena fe y de modo diligente, investigaciones voluntarias por iniciativa propia con el fin de detectar, identificar y retirar contenidos ilícitos o bloquear el acceso a éstos, pudiendo acogerse igualmente al régimen de exención de responsabilidad previsto con carácter general en los artículos 4 a 6 RSD.

4.2. Obligaciones de diligencia debida de los prestadores de servicios de alojamiento de datos, en particular plataformas en línea de comercio electrónico.

Las condiciones que delimitan el régimen de exención de responsabilidad de los servicios intermediarios, en especial los de alojamiento de información, deberán ser interpretadas ahora a la luz de las obligaciones de diligencia debida ("*due diligence*") introducidas por el Reglamento de Servicios Digitales para crear un entorno en línea transparente y seguro, con la finalidad de prevenir y corregir con prontitud posibles infracciones de derechos de terceros por parte de los usuarios profesionales de la plataforma. Obligaciones de diligencia que constituyen -sin duda- una de las principales y más reseñables novedades de la normativa aplicable a los servicios de intermediación en el nuevo Reglamento de Servicios Digitales, junto a las reglas que establecen una estructura de gobernanza para garantizar la cooperación y la coordinación entre las autoridades competentes de los Estados miembros y la Comisión europea en cuanto a la supervisión y la exigencia del cumplimiento de esas obligaciones de diligencia debida.

Entre las obligaciones de diligencia debida destaca la obligación para los servicios de alojamiento de datos de establecer mecanismos internos sencillos de notificación y acción, de fácil acceso y manejo, para la comunicación electrónica de denuncias de contenidos u ofertas presuntamente ilícitas por parte de los usuarios finales del servicio (artículo 16 RDS), otorgando prioridad a las notificaciones que realicen los denominados "alertadores fiables", las cuales deberán tramitar y resolver sin dilaciones (artículo 22 RSD). De tal manera, lo que bajo el régimen de la DCE 2000 era meramente voluntario, ahora se convierte en un mecanismo obligatorio para los intermediarios de "*hosting*" en el RSD 2022.

Los intermediarios de alojamiento de datos, entre los que se encuentran las plataformas digitales, deben facilitar el envío de notificaciones suficientemente precisas y adecuadamente fundamentadas. Se considerará que las notificaciones enviadas proporcionarán un conocimiento efectivo o permitirán ser consciente del elemento de información de que se trate, cuando permitan a un prestador diligente de servicios de alojamiento determinar, "sin un examen jurídico detallado"[33], que la información o la actividad denunciadas

[33] Con ello parecen compartirse posibles responsabilidades en la retirada de contenidos, sobre todo en aquellos casos donde sea más complejo realizar una adecuada ponderación de derechos e intereses, como sucede con los conflictos entre libertad de expresión e información con el derecho a la privacidad, el honor y la intimidad. De modo que los terceros afectados tienen la carga legal de facilitar la comprensión y valoración del conflicto a la plataforma digital, la cual tendrá más fácil no atender solicitudes de retirada de

son ilícitas (artículo 16.3 RSD) y, en consecuencia, reaccionar con prontitud para retirarla de su plataforma y bloquear su carga ulterior. El intermediario enviará un acuse de recibo y notificará, sin dilación indebida, su decisión respecto a la retirada o no de la información, incluyendo información sobre las vías de recurso de su decisión (artículo 16.4 y 5 RSD).

El prestador del servicio que aprecie la ilicitud o ilegalidad de informaciones, contenidos o actividades ofrecidos desde su plataforma deberá establecer restricciones a su visibilidad, incluida la eliminación de contenidos, el bloqueo del acceso a los mismos o su relegación, además de la cesación, suspensión u otra restricción de los pagos monetarios, la suspensión o cesación total en la prestación del servicio de intermediación, y la suspensión o supresión de la cuenta del destinatario, ofreciendo al usuario afectado una explicación clara sobre su decisión y los hechos y circunstancias que la hubieran motivado, incluyendo si actuó previa notificación de un tercero o por su propia iniciativa (artículo 18 RSD). Para ello, el intermediario deberá emitir una declaración de motivos clara y específica dirigida a los destinatarios de su servicio de intermediación en relación con su decisión de bloqueo o restricción de visibilidad de contenidos o informaciones ilícitos, suspensión o cesación total o parcial del servicio, suspensión o supresión de la cuenta del destinatario, incluyendo información clara y precisa sobre vías de recurso de su decisión, a través de mecanismos internos de reclamaciones, órganos de resolución extrajudicial de litigios y recursos judiciales (artículo 17 RSD).

A tal fin, todo intermediario en línea de alojamiento de datos tendrá la obligación de mantener un sistema interno de gestión de reclamaciones eficaz, electrónico y gratuito que permita a los usuarios afectados por una decisión de retirada o bloqueo de informaciones, o de suspensión o cesación total en la prestación del servicio de intermediación, la interposición de reclamaciones por vía electrónica y gratuita, debiendo notificar su decisión motivada sin dilaciones y la posibilidad de recurrir a un mecanismo de solución extrajudicial de conflictos o a los órganos jurisdiccionales competentes (artículos 20 y 21 RSD).

Por su parte, los Estados miembros deberán implementar mecanismos de resolución extrajudicial de litigios (conflictos) por un órgano certificado al efecto por el coordinador de servicios digitales nacional, cuyas decisiones no serán vinculantes para las partes (artículo 21 RSD). Los Estados miembros solo están obligados a cumplir con esta obligación gobernanza que supone el nombramiento de un coordinador de servicios digitales y el organismo de resolución extrajudicial de conflictos antes de la plena aplicación del RSD, el 17 de febrero de 2024.[34] Sin embargo, dado que la Comisión europea implementó sus funciones de ejecución para plataformas digitales y motores de búsqueda de gran tamaño el día 25 de abril de 2023, y considerando que es necesario contar con la asistencia y cooperación de las autoridades nacionales de los Estados miembros, decidió promulgar la Recomendación (UE) 2023/2425 de 20 de octubre de 2023, sobre la coordinación de respuestas a incidentes,

informaciones y contenidos cuando las denuncias recibidas sean imprecisas, salvo -entiendo- en los casos donde la infracción de los derechos de terceros sea evidente a la luz de las circunstancias.

[34] No se ha previsto nada aún en nuestro país sobre cuál puede ser este órgano de resolución de conflictos, de modo que el Ejecutivo puede optar bien por crear un órgano "*ad hoc*" para resolver los conflictos relacionados con la retirada de contenidos, informaciones o actividades por parte de los intermediarios en línea, o bien por habilitar esta función en el seno de algún organismo ya existente (como la CNMC).

especialmente los derivados de la difusión de contenido ilícito, en anticipación a la plena entrada en aplicación del Reglamento 2022/2065 (Reglamento de Servicios Digitales)[35].

Por lo demás, más allá de la obligación de implementar los mecanismos de denuncia, retirada y bloqueo ("*notice & take down & stay down*"), se establece que las plataformas digitales deberán suspender -durante un periodo razonable y después de haber realizado una advertencia previa- la prestación de su servicio a los usuarios que proporcionen con frecuencia contenidos manifiestamente ilícitos (artículo 23.1 RSD); como deberán suspender igualmente la tramitación de avisos y reclamaciones a las personas físicas o jurídicas que envíen con frecuencia avisos o reclamaciones que sean manifiestamente infundados (artículo 23.2 RSD). En sus condiciones de uso, los intermediarios expondrán de manera clara y detallada su política respecto de usos indebidos de usuarios y terceros reclamantes (artículo 23.4)[36].

Por último, el Reglamento contiene una serie de reglas especiales en forma de obligaciones adicionales de gestión de riesgos sistémicos para prestadores de plataformas en línea y motores de búsqueda en línea de muy gran tamaño ("*gatekeepers*" o guardianes de acceso; cfr. artículos 33 y ss. RSD), que resultan especialmente importantes desde el punto de vista de la prevención por lo que se refieren a la evaluación diligente de riesgos sistémicos que deriven del diseño y funcionamiento de su servicio (artículo 34 RSD) y, sobre todo, con la obligación de aplicar medidas de reducción de riesgos razonables detectados en su sistema teniendo en cuenta especialmente las consecuencias de esas medidas sobre los derechos fundamentales (artículo 35 RSD)[37].

Esta última obligación sugiere la posibilidad de implementar medidas o técnicas de reconocimiento automático de contenidos potencialmente ilícitos para facilitar su posterior retirada, en caso de comprobar su manifiesta o más que probable ilicitud. Técnicas estas que, realmente, estarían matizando o

---

[35] C(2023) 7170. DO L de 26 de octubre de 2023. En realidad, con esta solución provisional la Comisión europea busca una respuesta rápida y activa, coordinada y coherente, de los Estados miembros a los incidentes derivados de la difusión de contenido ilícito en plataformas digitales de muy gran tamaño que planteen un claro riesgo de intimidación a determinados grupos de población y de desestabilizar las estructuras políticas y sociales en la Unión o en parte de ella, incluido el contenido que pueda constituir una amenaza grave para la seguridad pública o la salud pública (en particular los contenidos relacionados con la guerra entre Rusia y Ucrania y Hamás e Israel). Aunque seguramente servirá de excusa para incentivar la designación rápida de un Coordinador de Servicios Digitales y la participación en la red de cooperación con la Comisión.

[36] Esta posibilidad de suspender el servicio a los usuarios especialmente o reiteradamente ofensivos y de no tramitar denuncias poco o escasamente fundadas puede ser muy importante en la práctica para las plataformas digitales en el caso de reclamaciones por comentarios presuntamente ofensivos o injuriosos, a la vista del elevadísimo número de comentarios insultantes que pueden encontrarse en foros digitales y redes sociales, así como al previsiblemente frecuente número de denuncias con que pueden encontrarse por parte de los afectados. Será determinante el contenido más o menos preciso de la reclamación que realice el afectado y que evite a la plataforma tener que realizar una compleja ponderación de derechos.

[37] Destaca especialmente en la protección de derechos de la personalidad (privacidad), lo previsto en el artículo 35 letra k): la adopción de medidas adecuadas para "*garantizar que un elemento de información, ya se trate de imagen, audio o vídeo generado o manipulado que se asemeja notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puede inducir erróneamente a una persona a pensar que son auténticos o verídicos, se distinga mediante indicaciones destacadas cuando se presente en sus interfaces en línea y, además, proporcionar una funcionalidad fácil de utilizar que permita a los destinatarios del servicio señalar dicha información*". De este modo las grandes plataformas y motores de búsqueda están obligados legalmente a actuar de manera especialmente diligente en la vigilancia, detección e identificación de ultrafalsificaciones o "*deepfakes*", lo que facilitará a su vez su rápida retirada por la propia plataforma o a instancia de las personas afectadas.

relativizando para las grandes plataformas la prohibición -establecida en el derogado artículo 15 DCE y el vigente artículo 8 RSD- de vigilancia o monitorización o búsqueda activa de hechos o circunstancias que indiquen la existencia de actividades ilícitas en su sistema, pero que a su vez entroncan con la posibilidad de realizar investigaciones propias y en cumplimiento del Derecho prevista en el artículo 7 RSD; máxime cuando el cumplimiento del Derecho en cuestión viene obligado por el mismo RSD para las grandes plataformas y motores de búsqueda de muy gran tamaño en relación con riesgos sistémicos que deriven del diseño y funcionamiento de sus servicios (como puede suceder, en particular, con las redes sociales en relación con posibles infracciones de derechos a la intimidad, el honor o la imagen).

A la postre, conjugar la prohibición del artículo 8 RSD con las medidas voluntarias del artículo 7 RSD y las obligaciones para grandes plataformas de los artículos 34 y 35 RSD, requiere un cuidadoso diseño y aplicación de las técnicas de reconocimiento automatizado de contenidos o informaciones, lo que exige salvaguardar en todo caso los derechos de los usuarios, primero con un diseño o ajuste estricto de ese tipo de técnicas de reconocimiento al reconocimiento de los supuestos de infracción más evidentes y socialmente alarmantes, y segundo, con una aplicación rigurosa de los mecanismos de recurso a favor de los usuarios y, llegado el caso, la rápida reposición de los contenidos e informaciones indebidamente retirados[38].

En definitiva, aunque el Reglamento de Servicios Digitales reitera el principio de inexistencia de un deber general de supervisión a priori, establece la obligación de implementar mecanismos de denuncia ("*notice, take down & stay down*") que servirá de prueba del despliegue de una diligencia debida en caso de enfrentarse a demandas de responsabilidad por infracciones de derechos de terceros cometidas por los usuarios de su servicio de intermediación. Establece asimismo la obligación para estos intermediarios de implementar mecanismos internos de recurso contra sus decisiones de retirada, bloqueo, suspensión o cesación de su servicio a los usuarios presuntamente infractores de derechos de terceros. Y establece, finalmente, la obligación de las plataformas y motores de búsqueda de muy gran tamaño de aplicar medidas de reducción de los riesgos razonables propios de su modelo de negocio y, por tanto, del diseño y funcionamiento de su servicio. Con lo cual, al tiempo que garantiza una mejor detección de contenidos, informaciones o actividades ilícitas, concretando la forma de tomar conocimiento efectivo por el intermediario, el legislador de la Unión incrementa notablemente el deber reacción diligente de las plataformas en línea en caso de recibir un aviso de infracción por parte de los titulares de derechos afectados por los contenidos, informaciones y actividades de su plataforma (que será especialmente frecuente en el caso de derechos de la personalidad), a modo de deber de supervisión a posteriori y específico. Los

[38] En relación con esta cuestión, pero en el contexto de la retirada de contenidos infractores de derechos de autor y conexos, comentando los equilibrios enfatizados por la STJUE de 26 de abril de 2022 (Asunto C_401/19, "República de Polonia c. Parlamento Europeo y Consejo de la Unión Europea") en relación con el artículo 17 de la Directiva 2019/790, del Parlamento Europeo y del Consejo, de 17 de abril de 2010, sobre los Derechos de Autor y Derechos Afines en el Mercado Único Digital, vid. LÓPEZ RICHARD, J., "Sistemas de reconocimiento automatizado de contenidos y ponderación de derechos fundamentales: el difícil equilibrio en la transposición del artículo 17 DDAMUD", en López Richard, J. y Saiz García, C. (Coords.), Digitalización, acceso a contenidos y propiedad intelectual, Dykinson, S.L., 2023, pp. 137-186.

intermediarios en línea deberán así evitar reacciones precipitadas a denuncias o notificaciones de terceros con escaso fundamento. Por el contrario, deberán buscar en sus decisiones un equilibrio entre los derechos de terceros (muy especialmente en el caso de los derechos al honor, la intimidad y la propia imagen, así como el tratamiento indebido de datos personales) y los derechos de sus usuarios (libertad de expresión e información).

Solo si extreman su diligencia en la forma establecida en el Reglamento de Servicios Digitales, podrán los intermediarios de alojamiento de datos y plataformas digitales exonerar su responsabilidad ante posibles infracciones de derechos de terceros cometidas por los usuarios de su servicio.

5. Naturaleza de la responsabilidad de los intermediarios en línea. En particular, su posible responsabilidad por intromisiones en la privacidad.

5.1. Consideraciones previas sobre la clase de responsabilidad imputable a las plataformas digitales.

De la jurisprudencia dictada al hilo de la interpretación del régimen de puertos seguros previsto en la DCE e incorporado en la LSSICE no queda claro cuál puede o debe ser el criterio o título de imputación de esa posible responsabilidad, pues ni el TS ni el TJUE han abordado directamente esta problemática.

En las sentencias dictadas hasta la fecha, los tribunales no se ocupan de la naturaleza de la posible responsabilidad en que puedan incurrir los servicios intermediarios de alojamiento de datos. Realmente el Tribunal no establece reglas de responsabilidad de los servicios de intermediación, sino -únicamente- las condiciones para que no se apliquen las reglas de puerto seguro o exención de responsabilidad de los intermediarios.

La Directiva de Comercio Electrónico no aclara nada al respecto, pero de su texto se deduce que los prestadores de servicios de intermediación responden por sus propias actividades y no por hechos ajenos[39]. Esto es, que su posible responsabilidad será por su comportamiento en el almacenamiento y difusión de contenidos propios o elaborados por él mismo o por cuenta suya, pero también por los actos destinados a facilitar, sin control alguno, las informaciones y actividades de los usuarios de su sistema, distinta por tanto de la responsabilidad que corresponda a los usuarios por los ilícitos cometidos contra derechos e intereses de terceros.

Por lo tanto, la responsabilidad de los operadores de redes y proveedores de acceso es una responsabilidad por hecho propio de índole subjetiva (el mismo

[39] Vid. APARICIO VAQUERO, "El nuevo régimen de prestación de servicios de la sociedad de la información", cit., p. 98. El único supuesto establecido en la norma de responsabilidad por hecho ajeno es aquel en que un usuario actúe bajo la dirección, autoridad o control del prestador del servicio de intermediación, en el caso de los prestadores de servicios de alojamiento (artículo 12.1 letra b. DCE; artículo 16.2 LSSICE) y prestadores de servicios de búsqueda (artículo 17.2 LSSICE), de forma similar a la responsabilidad del artículo 1903 CC. En contra, RUBÍ PUIG, "Derecho al honor online y responsabilidad civil de los ISPs", cit,, para quien la responsabilidad del intermediario es una responsabilidad por hecho ajeno (por las infracciones cometidas por los usuarios del servicio).

régimen de exención de responsabilidad excluye a priori una calificación de su responsabilidad como cuasi-objetiva u objetiva); cuestión distinta es que los datos o información causantes del daño a terceros provengan de terceros sujetos. Quiere esto decir que la responsabilidad civil, penal o administrativa no les será impuesta por el mero hecho de que un usuario profesional o particular del servicio de intermediación realice conductas que son o puedan considerarse ilícitas utilizando los servicios y recursos técnicos provistos por el intermediario (lo que nos llevaría a una responsabilidad objetiva por el mero riesgo que supone su actividad), sino por sus propias actuaciones en relación a tales conductas y la diligencia mostrada en evitarlas o impedirlas una vez conocidas[40]. Así pues, el intermediario de la sociedad de la información puede responder por acción u omisión propia en todo caso, pero -como se ha dicho ya- no responderá en ningún caso por el incumplimiento de una genérica obligación de supervisión de contenidos, que no puede exigírsele a priori por impedirlo el art. 15 DCE.

Pues bien, teniendo claro en todo caso que nunca se tratará de una responsabilidad vicaria o por hecho ajeno, sino que serán siempre supuestos de responsabilidad propia del intermediario derivada de su actuación no neutral o negligente (en caso de no reaccionar con prontitud para la retirada de contenidos ilícitos), la naturaleza y -por consiguiente- el título de imputación de responsabilidad a las plataformas digitales por las infracciones cometidas por los usuarios de su servicio debería determinarse en principio por las reglas de responsabilidad nacionales, o, en su caso, por conceptos autónomos del Derecho de la UE.

Llegados a este punto, es preciso decidir si la responsabilidad imputable, en su caso, a los intermediarios de servicios de alojamiento, incluyendo las plataformas en línea, es una responsabilidad indirecta por contribuir con su actividad a la infracción de derechos de terceros cometida por los usuarios de su plataforma, o si se trata más bien de una responsabilidad directa por el mismo concepto infractor que cometan los usuarios de su servicio; a saber, infracciones marcarias, contra derechos de autor o conexos, contra derechos de los consumidores o usuarios, intromisiones en el honor, la intimidad o la propia imagen, o tratamiento ilegítimo de datos personales.

La cuestión de fondo, entonces, es si los perjudicados pueden exigir al servicio intermediario (la plataforma digital) la misma responsabilidad que podrían exigir a los usuarios de la plataforma infractores de sus derechos, en el caso de la responsabilidad directa. O si, por el contrario, sólo podrían exigir una responsabilidad indirecta o secundaria ("*secondary Liability*") por contribuir o facilitar esas infracciones de derechos ("*contribution infringement Liability*") que debería reconducirse al esquema general de la responsabilidad civil extracontractual.

En la STJUE de 2 de abril de 2020 (Asunto C-567/18, "Coty Germany c. Amazon Services"), la cual versa sobre una cuestión prejudicial en materia de infracción marcaria por un vendedor de la plataforma "*Amazon Marketplace*"

[40] BUSTO LAGO, "La responsabilidad civil de los prestadores de servicios de la sociedad de la información (ISPs)", cit., pp. 1002 y ss., habla al respecto de los principios de "autorresponsabilidad", "cooperación" y "reacción diligente", por más que lo reconduce a supuestos de responsabilidad por hecho ajeno, *ex* artículo 1903 CC.

que se prevale de los servicios de promoción, almacenamiento y envío proporcionados por "*Amazon Logistics*", el Tribunal rechazó que pudiera apreciarse una infracción directa del derecho de marca por parte de Amazon en virtud de lo previsto en el artículo 9.3 b) del Reglamento (UE) 2017/1001, de 14 de junio de 2017, sobre la marca de la UE, el cual -dice- ha de interpretarse en el sentido de que debe considerarse que una persona que tiene en depósito por cuenta de un tercero productos que infringen un derecho de marca, sin tener conocimiento de esta infracción, no almacena estos productos con el fin de ofrecerlos o comercializarlos en el sentido de estas disposiciones cuando no persigue ella misma estos fines[41].

Sin embargo, en la STJUE (Gran Sala) de 22 de diciembre de 2022 (Asuntos acumulados C-148/21 y C-184/21, "Louboutin c. Amazon") el Tribunal se aparta del criterio propuesto por el Abogado General, estableciendo una nueva doctrina más garantista para los titulares de derechos de marca al disponer que cuando el operador de un sitio de venta en línea que integra, además de sus propias ofertas de venta, un mercado electrónico utiliza él mismo un signo idéntico a una marca de la Unión ajena, para productos idénticos a aquellos para los que está registrada la marca, cuando terceros vendedores ofrecen para su venta en dicho mercado, sin el consentimiento del titular de la marca, tales productos provistos de ese signo, si un usuario normalmente informado y razonablemente atento de ese sitio establece un vínculo entre los servicios de ese operador y el signo en cuestión, lo que ocurre, en particular, cuando, habida cuenta de todos los elementos que caracterizan la situación, ese usuario podría tener la impresión de que es ese operador quien comercializa, él mismo, en su propio nombre y por cuenta propia, los productos provistos de ese signo.

Es decir, el TJUE sanciona un régimen de responsabilidad directa de la plataforma digital de comercio electrónico por infracción de marcas ajenas, entendiendo que se produce un uso no autorizado de las mismas por las plataformas híbridas que entremezclan sus propias ofertas de venta con las ofertas de los vendedores o usuarios profesionales de su servicio de plataforma mediante una presentación uniforme de todas ellas incluyendo su propio logotipo de renombre en todos los anuncios, empleando reclamos comunes ("las mejores ventas", "las mejores ofertas"), contestando en común a preguntas de los usuarios demandantes sobre los productos, y prestando servicios de almacenamiento, envío y gestión de las devoluciones sin distinguir entre productos propios y ajenos (cfr. apartados 51 a 53). De modo que la infracción directa de marcas de terceros por el uso no autorizado de las mismas es cometida tanto por los usuarios profesionales como por la plataforma que

[41] Sin embargo, el Abogado General Manuel Sánchez-Bordona sí que entró al fondo de esta cuestión en las Conclusiones presentadas con fecha de 28 de noviembre de 2019, donde además de afirmar la responsabilidad directa de Amazon por su actividad logística en el depósito y envío de mercancías vendidas por usuarios de su plataforma infringiendo derechos de marca de terceros, sugiere también la vía alternativa de la responsabilidad indirecta de la plataforma como intermediario de la sociedad de la información que no actúa de forma neutral, automática y pasiva, poniendo de manifiesto en ambos casos que la destacada implicación de las plataformas en línea que gestionan mercados electrónicos en la comercialización de productos provoca que se les pueda demandar un "*especial esmero (diligencia) respecto del control de la licitud de los bienes con los que comercian*"; precisamente porque las plataformas digitales son o deberían ser conscientes de que, sin ese control, es fácil que sirvan de cauce a la venta de productos ilícitos que vulneran derechos de propiedad de terceros, no pueden, sin más, descargarse de su responsabilidad atribuyéndosela en exclusiva al vendedor (cfr. apartado 82 de las Conclusiones).

da cobertura a sus ofertas como si fueran propias. Aunque no se puede hablar de una responsabilidad directa y objetiva, pues la infracción se hace depender de una serie de condiciones o criterios que deberán ser apreciados en cada caso concreto por los jueces y tribunales nacionales competentes[42].

En definitiva, el TJUE establece las condiciones para poder diferenciar entre infracciones directas e infracciones indirectas a la hora de examinar la posible responsabilidad de las plataformas en línea, de manera que habrá una infracción directa de derechos de terceros cuando la plataforma realice por sí misma una conducta tipificada dentro de un derecho exclusivo de propiedad intelectual (marcas, derechos de autor y conexos), o resulte responsable directa -como editora- de información que atente contra la intimidad, el honor o la propia imagen, que no respete la normativa sobre datos personales o que no respete las normas de protección de consumidores y usuarios; mientras que habrá una infracción indirecta cuando contribuya a la infracción de derechos de terceros por parte de los usuarios de su servicio, bien porque no implementa ningún mecanismo eficaz de denuncia y retirada o bloqueo para impedir la infracción de esos derechos de terceros siendo o debiendo ser consciente de que se están produciendo, porque implementando esos mecanismos o teniendo conocimiento por cualquier otro medio de contenidos ilícitos no reacciona con prontitud para retirarlos, o bien porque estimula, incita o incluso controla esos comportamientos infractores.

5.2. La responsabilidad aplicable a las plataformas digitales en casos de intromisiones en la privacidad.

La alusión genérica a intromisiones en la privacidad incluye tanto las infracciones por intromisión en el honor, la intimidad o la propia imagen de terceros, así como en el tratamiento ilegítimo de datos personales. El concepto anglosajón de privacidad ("*Privacy*") hace referencia a cualquier ámbito de la vida privada que se tiene derecho a proteger frente a posibles intromisiones o utilizaciones inconsentidas[43], incluyendo no sólo la intimidad, la imagen o cualquier situación que afecte al honor, sino también la utilización de datos personales. Así, mientras la intimidad hace referencia a las esferas de mayor reserva privada de una persona, libre de cualquier injerencia pública, el concepto más amplio de privacidad incluye toda información relativa a una persona que puede servir para su identificación. En este contexto, la protección

[42] A diferencia de lo establecido por el mismo Tribunal en materia de infracciones directas de derechos de autor y derechos conexos por parte de las plataformas digitales que permiten a los usuarios compartir contenidos en línea, conducta fue considerada por la STJUE de 14 de junio de 2017 (Asunto C-610/15, "The Pirate Bay"), como un acto de puesta a disposición en línea sujeto al derecho exclusivo de autores, intérpretes y productores (artículo 3 de la Directiva 29/2001/CE, de 22 de mayo, sobre derechos de autor y derechos afines en la sociedad de la información) por parte de la propia plataforma prescindiendo por completo de su condición de intermediario en línea, provocando el cambio normativo plasmado luego en el artículo 17 de la Directiva 2019/790, de 19 de abril, sobre derechos de autor y derechos afines en el mercado único digital (cfr. artículo 73 del Real Decreto-Ley 22/2021, de 2 de noviembre). Vid. CARBAJO CASCÓN, F., "Las plataformas digitales ante la distribución de mercancías y el suministro de contenidos digitales ilícitos", cit., pp. 22 y ss.

[43] El artículo 12 de la Declaración Universal de los Derechos Humanos, se refiere a la privacidad como el derecho a que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

de datos personales no es en rigor un derecho de la personalidad pero sí que se incluye, obviamente, en una tutela más amplia de la privacidad, pues tiene como objeto garantizar a las personas naturales el control de toda información relacionada con su persona y actividades frente al tratamiento por parte de terceros.

El servicio de intermediación en línea responderá directamente frente a los afectados cuando esa intromisión tenga su origen en información o contenidos generados por el propio intermediario (en el caso de plataformas o servicios de intermediación mixtos o híbridos, como puede ser el caso de diarios y revistas digitales que ofrecen al mismo tiempo foros de opinión y comentarios). En tales casos los afectados podrán dirigir contra el servicio en línea las acciones previstas en la legislación española en la Ley Orgánica 1/1982, de 5 de mayo (artículo 9.2). Lo mismo puede decirse cuando la plataforma digital lleve a cabo un tratamiento ilegítimo de datos personales, estando a lo dispuesto en la normativa de la Unión y de los Estados miembros sobre protección de datos personales y sin perjuicio de solicitar indemnizaciones por la vía de la responsabilidad extracontractual del artículo 1902 CC.

Sin embargo, la responsabilidad del intermediario será indirecta en el caso de tener conocimiento efectivo por cualquier medio (fundamentalmente mediante denuncias o notificaciones realizadas por el afectado en el canal interno de reclamaciones de la plataforma) de contenidos, actividades o informaciones suministrados por los usuarios de su servicio[44] que vulneren o puedan vulnerar el derecho al honor, a la intimidad o a la propia imagen de terceros, o por el tratamiento ilícito de datos personales, y no reaccione con prontitud para retirar esa información y bloquear el acceso posterior de la misma a la plataforma; lo que incluye, como se dice en la STJUE de 3 de octubre de 2019 (Asunto C-18/18, "Eva Glawischnig Piesctek v. Facebook"), la obligación no sólo de retirar o bloquear el acceso a la información suministrada por un concreto usuario identificada en la denuncia o notificación del tercero afectado ("*notice & take & stay down*"), sino también la de suprimir o impedir el acceso a cualesquiera otros datos o informaciones cuyo contenido sea idéntico al de una información declarada ilícita con anterioridad, sea quien fuere el autor de la solicitud de almacenamiento de tales datos, lo que incluye la obligación de implementar sistemas de filtrado y reconocimiento automatizado de contenidos o informaciones que sean idénticos al de una información declarada ilícita con anterioridad o a bloquear el acceso a los mismos, sea quien sea el responsable de la solicitud de almacenamiento de los mismos.

De modo que si el intermediario tiene conocimiento efectivo por cualquier medio -en particular por notificaciones o comunicaciones de los afectados, pero también por la implementación de mecanismos o técnicas de reconocimiento automatizado de contenidos ilícitos- de informaciones, contenidos o comentarios compartidos por usuarios de su servicio que vulneran el derecho al honor, la intimidad o la propia imagen de terceros, o un tratamiento ilegítimo de datos personales, y no reacciona de forma diligente y rápida para retirarlos o bloquear su acceso, podrá ser objeto de una demanda de responsabilidad civil

[44] Tanto quienes sean autores o responsables directos de las informaciones infractoras como los que contribuyan a su difusión realizando valoraciones personales también negativas podrán ser perseguidos por los terceros afectados, civil y penalmente (injurias y calumnias), en caso de poder ser identificados.

por el tercero afectado; responsabilidad civil, no por la infracción directa por el intermediario de esos derechos de la personalidad o privacidad, sino por contribuir a la infracción al poner los medios para facilitar posibles intromisiones en el honor, la intimidad, la propia imagen o el tratamiento ilegítimo de datos personales de terceros y no reaccionar con prontitud para retirar la información o contenidos infractores cuando tenga conocimiento efectivo de su existencia en su servicio o plataforma, lo que obligaría al afectado a ejercitar acciones contra el intermediario con fundamento en la cláusula general del derecho de daños, artículo 1902 CC, y no en la LO 1/1982 de 5 de mayo o en la normativa sobre protección de datos personales (que sí podrá aplicarse contra la plataforma digital en forma de denuncias ante la Autoridad nacional de protección de datos). Es así porque realmente es el usuario y no la plataforma quien comete una intromisión en la privacidad, honor o imagen del tercero, o quien hace una difusión no autorizada de datos personales, pero la vulneración de derechos de terceros se produce por la falta de neutralidad, en su caso, o falta de reacción diligente de la plataforma en caso de tener conocimiento de esas infracciones.

En definitiva, la exención de responsabilidad o la imputación de responsabilidad indirecta de los intermediarios en línea por infracciones de derechos de la personalidad, deberá valorarse caso por caso a la luz del mayor o menor grado de cumplimiento de sus obligaciones de diligencia debida en la forma de trabar conocimiento efectivo sobre la existencia de posibles infracciones y en la motivación sólida de su reacción diligente al retirar contenidos e informaciones, bloquear su acceso presente y futuro o, en los casos más graves, en la suspensión o cese definitivo del servicio al usuario infractor.

Lógicamente, cuanto mayor relevancia pública tenga la persona y más evidente sea la intromisión en su honor, intimidad o propia imagen, así como el uso no autorizado de sus datos personales, mayor celeridad debe mostrar la plataforma (especialmente en el caso de las redes sociales) para retirar la información e impedir que vuelva a subirse y para cesar en la prestación del servicio al responsable o responsables. Si la persona afectada es pública pero no es tan clara la intromisión en la privacidad, la plataforma debe realizar un cuidadoso análisis de ponderación entre la libertad de expresión e información y la afectación de derechos de la personalidad y datos personales. Y cuando el afectado no tenga relevancia pública esa ponderación de derechos debe inclinarse a favor del mismo si la intromisión en su honor, intimidad o utilización de la imagen o datos personales carece de sentido para la información o contenido que se está difundiendo por los usuarios.

Ahora bien, en el caso de plataformas o motores de búsqueda de muy gran tamaño habría que valorar si la infracción de lo dispuesto en los artículos 34 y 35 RSD, al no implementar sistemas que permitan la evaluación y reducción de riesgos de infracción de derechos de terceros cuando estos son sistémicos a la vista del diseño y aplicación de su plataforma o servicio, podría derivar en una responsabilidad directa -en lugar de indirecta- por facilitar con su negligencia infracciones reiteradas de derechos de terceros, como pueden ser muy especialmente los derechos de la privacidad o personalidad en servicios de redes sociales o similares.

Nivarra L, 'Artificial intelligence and infringement of intellectual property' (2024) 2 EJPLT, 84 – 101.
DOI: https://doi.org/10.57230/EJPLT242LN

EJPLT
ISSN 2704-8012



Artificial intelligence and infringement of intellectual property

LUCA NIVARRA
Full Professor of Private Law
University of Palermo

Abstract

This paper explores the intersection of artificial intelligence (AI) and intellectual property (IP), focusing on the challenges and implications of extending copyright protection to AI-generated works. It examines the debate on whether outputs generated by AI, without direct human intervention, qualify as intellectual works deserving copyright protection. The analysis addresses the circular reasoning that restricts originality to human authorship and proposes a framework that decouples creativity from human origin. Additionally, the paper discusses the implications of machine learning (ML) training on copyright, suggesting pragmatic solutions to incorporate AI-generated works into the realm of protectable IP. The paper argues for a shift from traditional copyright to contract law to address the economic rights associated with AI-generated works. This approach is essential to adapt to the evolving landscape of AI-driven creativity and the emerging market for AI-created intellectual works.

*This article was presented at the International Conference "*L'informazione ed il diritto*", 29-30-31 May 2024, Università Federico II, Orientale, Parthenope, Suor Orsola Benincasa, Napoli.
Scientific Committee: Prof. Francesco Romeo (Uni Federico II Napoli), Prof.ssa Vania Maffeo (Uni Federico II Napoli), Prof.ssa Roberta Montinaro (Uni Orientale Napoli), Prof. Roberto Carleo (UNI Parthenope), Prof. Agostino De Caro (Uni Molise), Prof. Giuseppe Di Chiara (Uni Palermo), Prof.ssa Lucilla Gatt (Uni Suor Orsola Benincasa), Prof. Mariano Menna (Uni Campania).

© The author(s) 2024, 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: IP; copyright; artificial intelligence; machine learning; infringement

Summary: 1. AI creations. – 2. IA and inputs. – 3. IA and outputs. – 4. IA and intellectual property: more than just an infringement. – 5. Production of intellectual works by means of intellectual works: from copyright to contract law.

1. AI creations.

A reliable exploration and development of the assigned topic requires some preliminary clarifications involving various levels of legal reasoning.[1] As is well known, the debate on intellectual property (IP) has fundamentally concerned the possibility of attributing the quality of intellectual works to outputs generated by AI in an entirely autonomous manner – thus not merely as instrumental support to the creative activity of a human creator – with the corresponding extension of copyright protection to such works. The arguments supporting the opposing theses, both contrary and favorable, develop on different levels. The former are based on the letter of the law (EU Directives, the Berne Convention, and national laws of many countries inside and outside the Union) and the case law of the Court of Justice (starting in particular from the Infopaq case). The latter rely on illustrating the effects (positive or negative) that would result from including or excluding AI-generated artifacts from the copyrightable domain.

At this initial stage, I will attempt to articulate an argument in favor of copyright protection for these works that is systematic in nature—not in the traditional sense, where the adjective denotes a legal reasoning aimed at ensuring consistency with the text to be interpreted,[2] but in a way that pertains to how law performs its task of regulating social processes. This means a systematicity not restricted to the legal system alone: a transversal systematicity, not merely vertical.

From this perspective, the contrary argument is untenable. It is based on a notion of originality confirmed by legislative texts and the Court of Justice, which require the work to result from the creative effort of its author, thus bearing unmistakable traces of the author's personality. [3] This close link

[1]This work is the result of a Report presented at the annual conference of the Unione dei Privatisti on "Il diritto privato nell'economia digitale", Università Cattolica del Sacro Cuore, Milano, 17 – 18 novembre 2023.
[2] For instance, it could be deduced from Article 111 of the Civil Code that marriage is a contract, but the system, including Article 1321 of the Civil Code, shows, on the contrary, that the use of the word 'contract' is limited to bilateral acts with patrimonial content; hence the problem of establishing what is meant by 'patrimonial', with the consequent inevitable involvement of Article 1174 of the Civil Code, which proves the circumstance that legal interpretation is essentially a systematic interpretation.
[3] On the legislative side, mention must be made of Directive 2009/24/EC (on software protection); Directive 96/9/EC (on database protection); Directive 2006/116/EC (on the term of protection of copyright and certain related rights). In particular, with regard to software (Recital 7 and Art. 1(3) of the Software Directive) and photographic works (Recital 16 and Art. 6 of the Term Directive), the European Union legislator has established, in terms of originality, that originality exists when the work is the "result of the author's own intellectual creation"; while with regard to databases (Recital 16 and Art. 3(1) of the Database Directive), the European Union legislator has established that originality exists when the work is the "result of the author's own intellectual creation", No. 16 and Art. 3(1) of the Database Directive), the work must be

between the subjective and objective aspects of originality implies that an original work requires an author, who must be a human being. However, this conclusion is flawed due to its circular reasoning. Qualities typical of human intelligence are postulated for an original work, and the attributes required for copyright protection are deduced from human intelligence characteristics.

Upon closer inspection, the weakness of this reasoning reveals a more serious issue, which affects the role of law in regulating social processes. The semantic status of the question concerning the protectability of works "created" by AI is descriptive, not prescriptive or deontological. This means that the correct way to formulate the question is: "Are works created by AI works of intellect (in italian: opere dell'ingegno)?" and not "Are AI-created works expressions of human creativity?"

To place the issue in the right perspective – even if only as a hypothesis or intellectual experiment – it is necessary to consider the possibility of disassociating the originality of the work from its human origin. This would break the link between "creative" and "human," exposing the logical fallacy behind the argument and the delusion of law's omnipotence.

I do not know if every discourse on AI, but certainly the discourse on AI and its legal regulation should start from an assumption that, in my opinion, cannot

---

considered original if it is "the author's own intellectual creation". Since the Infopaq judgment (Judgment of 16 July 2009, *Infopaq*, C-5/08, EU:C:2009:465), the Court of Justice has been working on a harmonisation of the requirement of originality/creativity, so to speak horizontal, i.e. of general scope, starting from Art. 2(a) Directive 2001/29/EC (on the harmonisation of certain aspects of copyright and related rights in the information society: the so-called Infosoc Dir. Infosoc) according to which "Member States shall provide the persons listed below with an exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction in any manner or form, in whole or in part". However, in the Court's view, since as is clear from recitals 4, 9, 10, 11 and 20 of dir. In the Court's view, since, as is clear from recitals 4, 9, 10, 11 and 20 of the Infosoc directive, the latter, in establishing a harmonised legal framework, cannot but be based on the same principle as the software, database and term directives, according to which, as we have seen, protection is subject to the circumstance that the work is original, that is to say, represents the result of the author's intellectual creation, it follows that the exclusive reproduction right established by Article 2(a) of the Infosoc directive cannot but apply to the reproduction right in the case of a work of authorship, and that the right of reproduction established by Article 2(a) of the Infosoc directive cannot but be protected by the same principle as the software, database and term directives. Infosoc can only apply to an object that is original, i.e. represents the result of the author's creative effort (paragraphs 35-37 of the Infopaq decision). Given these assumptions, since as regards newspaper articles (this was the type of work at issue in the dispute), the requirement of originality resides in the manner in which the subject matter is presented as well as in the linguistic expression, 'it cannot be excluded that certain isolated phrases or, even certain parts of sentences of the text in question, are capable of conveying to the reader the originality of a publication such as a newspaper article, by communicating to the reader an element which is in itself an expression of the intellectual creation of the author of that article' (paragraphs 44-47). Thus, even an excerpt of only 11 words that immediately and effectively conveys to the reader the meaning of the indexed article may constitute an original work. In short, the Court of Justice, through the medium of Art. 2(a) dir. In short, the Court of Justice, through the medium of Article 2(a) of the Infosoc Directive, subject, indeed, to a rather stretched reading, brings into the sky of general concepts the very basic notion of originality prepared by the European legislator with reference to certain specific types of intellectual works with a high technological density. A notion of originality that, ultimately, rests on the idea that the creative character of the work derives from the author's exercise of his freedom of choice as to the expressive form to be given to the artefact. It is quite peculiar that, by setting such a low threshold of originality (all the case law of the Court of Justice subsequent to Infopaq moves in this direction, starting with the equally famous Painer case (Judgment of 1 December 2011, *Painer*, C-145/10, EU:C:2011:798) in which the author's choice of subject matter, angle, light, etc. is sufficient to ensure the originality of the work, a photograph, in order to ensure the originality of the work), the author's choice of form is sufficient to ensure the originality of the work. For a thorough examination of the Court of Justice's guidelines, please refer to S Guizzardi, 'Il requisito della originalità delle opere dell'ingegno come armonizzato dalla Corte di Giustizia' (2020) AIDA 3 ff. See also, A Ramalho, 'Originality redux: an analysis of the originality requirement in AI-generated works' (2018) AIDA 23 ff.

be disputed: namely, that AI exposes a cognitive gap in law, not simply an axiological one. By this, I mean that the phenomenon of AI is radically new; it introduces a gap between the representation of the world underlying the legal enterprise and the reality on which it exercises its regulatory claim. Therefore, it cannot be tackled by simply reapplying the set of rules and principles accumulated in the past when discussing creativity was synonymous with discussing human creativity. Otherwise, one unduly converts an ontological problem into a deontological one, a conversion evident in the presumed inseparability of the creativity-human being nexus. This presumption, on a logical-linguistic level, is shown to be fallacious in light of the 'new world', as it can no longer be presupposed (hence its circularity) but demands, for the first time in history, to be proven.

In other words, the law is not qualified to answer negatively on the protectability of AI works simply because it lacks (or only apparently has) the necessary resources. The 'artificial,' historically a dominant trait of human activity, now, in its present-day manifestations, shows a tendency to substitute rather than merely assist its creator. Law must find reasonable solutions to this transition, which is as profound in content as it is uncertain in outcome.[4]

2. IA and inputs.

Once it is established that appealing to the *status quo* is conceptually inadequate, the problem can be addressed within the framework of law as a social subsystem providing services aimed at solving practical problems through the attribution of legal titles. This environment is suited for pragmatic or consequence-oriented arguments[5]. Works 'created' by AI can and do possess originality, whether they are literary works, figurative art, musical works, etc. Two strategies exist: (1) consider the true author as still human (e.g., the programmer) – preserving the basic infrastructure of authorial protection (the originality of the work and the tracing of an author). Or (2) fully separate the originality of the work from the author, attributing the ownership of economic rights to another subject (e.g., the user of the system, along the lines of the rule already tried and tested with regard to non-creative databases), with the consequence that the problem will no longer be that of identifying an author in the traditional sense of the term, but rather that of identifying a subject to whom the ownership of the rights of economic use of the work should be attributed. The real issue at stake is incorporating these works into the orbit of

[4] Speaking of 'artificial', an analogy that is perhaps not entirely peregrine can be found in artificial insemination. In that case, too, we were in the presence of a technology of reproduction that replaced the 'natural' one: but the 'natural' ceases to be so when it is joined by the 'artificial' or, at the very least, downgraded to a purely descriptive cognition of a possible (no longer the only) mode of reproduction of the species: so that, in that case too, the reference to 'nature' as a strategy for establishing limits and prohibitions took on an ideological connotation. The matter becomes more complex when the new technology is placed at the service of reproductive modalities that directly affect the social bond, or when the 'artificial' is an instrument of rewriting consolidated cultural codes, the defense or overcoming of which legitimately commits the right to a stance that can also be one of repulsion: emblematic, in this regard, is the case of surrogate motherhood in its various forms.

[5] See, in this respect, the relevant observations of S Guizzardi, 'La protezione d'autore dell'opera dell'ingegno creata dall'intelligenza artificiale' (2018) AIDA 42 ff.

the protectable, as opposed to allowing them to fall into the public domain. This latter outcome would be disastrous, primarily for those who hold rights to the intellectual works from which the AI has 'derived' its unique artifact.

The core issue is ML training – administering data (often consisting of intellectual works that have not yet fallen into the public domain) to AI systems for learning and self-correction (ML), resulting in outputs that may show originality. The paradox is that denying these AI works the status of 'intellectual works' opens a temporal gateway, an anticipated public domain, absorbing all 'first' intellectual works used for training. This situation undermines the control authors have over creative reworkings of their work. In other words, the defense of copyright's anthropocentric nature may ironically contribute to its crisis by undermining one of its core principles: the author's control over derivative works, which can only be asserted if those works are legally protected.

Conversely, it is also true that – as is pointed out by those who rely, in order to oppose the entry of AI-generated artefacts into the *sanctum sanctorum* of intellectual works, on an argument of a pragmatic and not merely ideological nature (inconsistent as we have seen) – the prodigious reproductive capacity of these systems risks bringing creativity to the point of collapse, saturating the market with 'serial' works of intellect (in production, not in content) and thus disincentivizing the creative effort of human authors. The paradox, therefore, becomes a dilemma: either penalize works feeding AI training, affecting past creativity, or discourage future creativity by competing with AI's serial production.

3. IA and outputs.

Generative AI fundamentally challenges the traditional dichotomy between idea and expressive form in authorship. Authorship protection is based on the assumption that, despite our species' rich endowment compared to other animals, we ultimately repeat ourselves. If intellectual works directly matched their inspirational themes, writing something original after the Iliad and the Odyssey would have been extremely difficult. Although we hold ourselves in high regard, our pursuits – war, power, money, love, personal affirmation, food, alcohol – tend to be repetitive. Thus, copyright protection focuses not on the theme itself but on its variation: the expressive form rather than the idea. This is seen in the forms of culture and their respective sign systems, such as literature, visual arts, and cinematography.

Historically, this framework was effective. The distinction between the idea (unprotected) and its artistic expression (protected) allowed for a basic yet effective defense based on the monopoly of reproduction, benefiting the author. The advent of digital technologies, enabling unlimited and cost-free copying, necessitated strengthened reproduction exclusivity, as reflected in the 2001 Infosoc Directive (Art. 2 and 5). Despite this, a copy remains a copy, regardless of how easily it is made. The protected status is firmly linked to physical reality, maintaining the idea/expression distinction's relevance.

However, in today's world, and likely even more so in the future, it is and will

be legitimate to harbor doubts about whether that distinction holds. AI systems, trained on vast amounts of data and capable of learning and self-correction, complicate the issue. When appropriately stimulated, these machines can produce outputs (e.g., drawings, photographs, stories) that are not mere copies – mainly due to the multitude of training inputs – but also not traditional creative re-elaborations (like film adaptations or translations). The connection to the original work is so diluted that the output only shares a family resemblance, a recognizable trait, a style.

It might be argued that there have always been works "in the manner of," with great artists having imitators inspired by their works and style. After all, it is a common opinion that style, however distinctive, does not fall under copyright protection, as this would extend copyright beyond its intended objectives. Yet, with AI, style reproduction becomes serial and increasingly sophisticated, reducing the distance from the original without constituting copying. In the hands of AI, the idea/expression dichotomy becomes opaque, undermining its reliability as a cornerstone of copyright protection discourse.

4. IA and intellectual property: more than just an infringement.

Of course, it may well be the case that through these learning and self-correction programs, the reproduction right is violated. Similar events occur when the data administered to the AI, instead of being disaggregated and then reassembled (non-expressive use), are memorized and returned to the end user in their original configuration (memorization).[6] This, in particular, may occur when the output reproduces a text or design that has been "passed" more than once during the training phase, thereby facilitating the memorization of the model and, consequently, its faithful reproduction. However, it does not seem to me that phenomena of this kind, involving clear infringement of intellectual property, represent the heart of the problem. To tell the truth, one sure way of turning a rather banal issue into a problem is precisely to deny AI outputs the dignity of works of intellect by consigning them to the inhospitable territory of the public domain.

At this point, in light of the brief remarks made so far, I would like to say something about the title of this report, "AI and Infringement of Intellectual Property": a title that seems a little misleading to me, for reasons we will immediately see. The history of intellectual property, and particularly the history of copyright, is a history of crises and correlative adaptations of various kinds, primarily legislative ones. These crises, which are closely linked first and foremost to the evolution of technology, but also to the influence that the progress of knowledge exerts on thought in general, and on the way of understanding art in particular, ultimately assume two basic postures.

In the first case, there is a direct attack on the prerogatives recognized to the author: from counterfeiting to reprography, up to the advent of digital technologies and then the internet, the essential core of the bundle of rights

[6] M Sag, 'Copyright Safety for generative AI' (2023) 2 Forthcoming in Houston Law Review, 61. Available at SSRN https://ssrn.com/abstract=4438593 or http://dx.doi.org/10.2139/ssrn.4438593.

constituting exclusivity has been constantly undermined, and in recent decades with increasing intensity, inducing legislators (national, supranational, international) to adopt measures either of hypertrophic reinforcement of exclusivity itself (the case of the reproduction right, already mentioned, is emblematic) or of retribution for creative effort of a lump-sum type (fair compensation).

In the second case, the crisis settles at the very heart of copyright, understood not only as an instrument to regulate certain phenomena but also as a device dedicated to transcribing these phenomena into the language of law. In other words, it is not only or not so much the effectiveness of copyright that is in crisis, but rather its cognitive attitude. This occurs every time it is overtaken by a particular way of behaving in the interweaving of technology, artistic thought, and forms of expression that undermine the categories used to interpret reality, causing radical disorientation.[7]

This has already happened, to cite an illustrious precedent, with conceptual art; and this is what is happening with AI and its unprecedented ability to create works that, through the decomposition and recomposition of the latent features characterizing a style, are located, as we have seen, exactly at the crossroads of idea and expressive form. This is why it seems to me that AI challenges the structure of copyright from the ground up. And this is also the reason why, in my opinion, the title of the report is somewhat misleading: because, in reality, what AI does to intellectual property is much more than undermining it in the traditional sense of the term; it literally disrupts it and forces a radical rethinking. A development such as AI, with the characteristics we have briefly recalled, cannot be harnessed within asphyxiating maneuvers to adjust the basic coordinates of copyright, because it is these that are in crisis.

5. "Production of intellectual works by means of intellectual works": from copyright to contract law.

There is one point on which there is substantial consensus among those who reject the idea that creativity can be separated from the human and deny AI-generated works the status of copyrightable works, and those who, conversely, see originality in AI outputs. Both agree that, at least with current technology, AI cannot function entirely independently; it requires input and the learning of a language to process those inputs autonomously. No one would think of denying the dignity of a work of intellect to a piece of writing endowed with the necessary and sufficient degree of originality (very low, as we have seen) just because the language in which it was composed is the one learnt by the author in primary school; nor because the writing intercepts and reinterprets material, style, and cultural traditions from the author's environment in an original way.

The creation of an AI-generated work involves a choice by the user, distinct from the choices leading to the creation of the output, and made by a different entity – the AI. This results in a split creative process: humans decide to create

[7] See G Ajani, 'Contemporary Artificial Art and Law. Searching for an Author' (2019) Art & Law, 1 ff.

the work, while the machine handles its elaboration. This division makes it difficult to establish the exact incidence of each contribution to the final output[8], and gives the work a new form, challenging traditional copyright frameworks.

The dominant role of AI in producing intellectual works has as a corollary that the input driving AI creation becomes also artificial. This parallels the deep transformation of the English economy during the Industrial Revolution in the 18th century, shifting from home workshops to the spinning mill and then to factories. Today, we are witnessing the production of intellectual works (output) by means of intellectual works (input), leading to a new market for AI-created works. This emerging market demands a regulatory solution that transcends the romantic paradigm of copyright protection, particularly the Euro-continental model, and embraces the perspective of industrial processes, necessitating an integrated legal approach.

The analogy with the Industrial Revolution and the capitalist transformation of the economy is particularly fitting here. Inputs – often still-protected works of intellect – represent a use value for which the user must pay a fee. It is impractical for these transactions to occur individually, as the costs would be prohibitive and it would be nearly impossible for individual authors to track their works used for AI training. Instead, collective negotiation by societies, with fees based on the quantity of output put on the market by each user and their turnover, could be a solution. This model, inspired by collecting societies and fair compensation in Copyright Law (Legge No. 633/1941), differs in that remuneration would be based not on the exclusive right to reproduce or rework the intellectual work, but on its use value for the user and, consequently, its exchange value for the author. The information obligations outlined in Article 110-quater of the Italian Copyright Law (Legge No. 633/1941) could also be borrowed and adapted. These obligations would require informing authors, through their collective management bodies, about the activities conducted and revenues generated by the user.

In short, this phenomenon should be viewed through the lens of contract law rather than copyright protection, a perspective already fairly widespread in scholarly opinion. Copyright protection will play a marginal role, confined to cases of blatant infringement. The system user, meanwhile, should consider themselves the owner of the economic rights to the work created by AI. In the downstream market, where the intellectual work (output) is considered an exchange value, copyright rules can be applied by default.

[8] G Rossi, 'L'intelligenza artificiale e la definizione di "opera dell'ingegno"' (2018) AIDA, 268 ss.

Nivarra L, 'Intelligenza artificiale e violazione della proprietà intellettuale' (2024) 2 EJPLT, 84 – 101.
DOI: https://doi.org/10.57230/EJPLT242LN

EJPLT
ISSN 2704-8012



Intelligenza artificiale e violazione della proprietà intellettuale

LUCA NIVARRA
Professore Ordinario di Diritto privato
Università degli Studi di Palermo

Abstract

Questo articolo esplora l'intersezione tra intelligenza artificiale (IA) e proprietà intellettuale (PI), concentrandosi sulle sfide e sulle implicazioni dell'estensione della protezione del copyright alle opere generate dall'IA. Esamina il dibattito sulla questione se gli *output* generati dall'IA, senza l'intervento diretto dell'uomo, possano essere considerati opere intellettuali meritevoli di tutela del diritto d'autore. L'analisi affronta il ragionamento circolare che limita l'originalità alla paternità umana e propone un quadro che disaccoppia la creatività dall'origine umana. Inoltre, il documento discute le implicazioni dell'apprendimento automatico (ML) sul diritto d'autore, suggerendo soluzioni pragmatiche per incorporare le opere generate dall'IA nel regno della proprietà intellettuale tutelabile. Il documento sostiene la necessità di passare dal diritto d'autore tradizionale al diritto contrattuale per affrontare i diritti economici associati alle opere generate dall'IA. Questo approccio è essenziale per adattarsi al panorama in evoluzione della creatività guidata dall'IA e al mercato emergente delle opere intellettuali create dall'IA.

* Questo articolo è stato presentato al Convegno interuniversitario "L'informazione e il diritto", 29-30-31 maggio 2024, Università Federico II, Orientale, Parthenope, Suor Orsola Benincasa, Napoli.
Comitato scientifico: Prof. Francesco Romeo (Uni Federico II Napoli), Prof.ssa Vania Maffeo (Uni Federico II Napoli), Prof.ssa Roberta; Montinaro (Uni L'Orientale Napoli), Prof. Roberto Carleo (UNI Parthenope); Prof. Agostino De Caro (Uni Molise), Prof. Giuseppe Di Chiara (Uni Palermo), Prof.ssa Lucilla Gatt (Uni Suor Orsola Benincasa), Prof. Mariano Menna (Uni Campania).

© The author(s) 2024, 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: proprietà industriale; copyright; intelligenza artificiale; machine learning; violazione

Summary: 1. Le opere dell'IA. – 2. L'IA e gli *input*. – 3. L'IA e gli *output*. – 4. IA e proprietà intellettuale: molto più che una semplice lesione. – 5. "Produzione di opere dell'ingegno per mezzo di opere dell'ingegno": dalla tutela d'autore al diritto dei contratti.

1. Le opere dell'IA.

Impostazione e svolgimento attendibili del tema assegnatomi richiedono alcuni chiarimenti preliminari che investono vari piani del ragionamento giuridico. Come è noto, il dibattito su IA e proprietà intellettuale ha riguardato, fondamentalmente, la possibilità, o meno, di attribuire alle opere dell'ingegno generate dalla prima in modo del tutto autonomo – e, quindi, non nella veste di mero supporto strumentale all'attività creativa di un artefice umano – la qualità di opere dell'ingegno, con correlativa estensione ad esse della tutela d'autore. Gli argomenti addotti a sostegno delle due tesi, quella contraria e quella favorevole, sono tra loro eterogenei, nel senso che essi si sviluppano su piani diversi: i primi, infatti, si alimentano del richiamo alla lettera della legge (Direttive dell'UE, convenzione di Berna, leggi nazionali di molti paesi dentro e fuori l'Unione) e della giurisprudenza della Corte di Giustizia (a partire, in specie, dal caso Infopaq); i secondi, viceversa, hanno un'inclinazione più orientata alle conseguenze, là dove si fanno forti della illustrazione degli effetti (positivi o negativi) che discenderebbero dalla decisione di includere o escludere gli artefatti dell'IA dall'area del *copyrightble*.

A questo primo stadio del mio contributo, proverò ad articolare un argomento favorevole alla tutela d'autore delle opere in questione di tipo sistematico: non nel significato tradizionale di sistematico, dove l'aggettivo designa un modo di procedere della ragione giuridica attenta ad assicurare la coerenza della soluzione proposta con un vincolo non riducibile alla lettera dell'enunciato da interpretare[9], ma in un significato diverso che attiene al modo in cui il diritto svolge il suo compito di regolazione dei processi sociali (quindi, si potrebbe dire, una sistematicità attingibile dalla considerazione dei vari sistemi deputati allo svolgimento di quel compito e non ristretta al solo sistema giuridico: una sistematicità trasversale e non semplicemente verticale).

Da questa prospettiva, l'argomento contrario si rivela palesemente insostenibile. Esso si fonda, come già osservato, su una nozione di originalità dell'opera dell'ingegno, asseverata dai testi legislativi e dalle pronunzie della Corte di giustizia, alla stregua della quale quest'ultima deve essere la risultante dello sforzo creativo del suo autore, cioè discendere dalle scelte che hanno

[9] Ad es. dall'art. 111 c.c. si potrebbe desumere che il matrimonio sia un contratto, ma dal sistema, comprensivo dell'art. 1321 c.c., si ricava, viceversa, che l'uso della parola "contratto" è circoscritta agli atti bilaterali a contenuto patrimoniale; donde, poi, il problema di stabilire cosa debba intendersi per "patrimoniale", con conseguente inevitabile messa in gioco dell'art. 1174 c.c., a riprova della circostanza che l'interpretazione giuridica è, essenzialmente, interpretazione sistematica.

presieduto alla sua elaborazione e così recare impresse le inconfondibili tracce della personalità di quello[10]. Ora, il nesso strettissimo che questo paradigma definitorio istituisce tra il profilo soggettivo e quello oggettivo della nozione di originalità accolta in sede normativa ha come conseguenza che, affinché vi sia un'opera dell'ingegno, è necessario che vi sia un autore e, ancora, che, stante le caratteristiche predicate del processo creativo, l'autore non possa che essere un individuo appartenente alla specie umana (*human being*).

Si tratta, però, di conclusione viziata da una patente circolarità. Dell'opera dell'ingegno si postulano qualità, riferite in primo luogo all'iter della sua creazione, tipiche dell'intelligenza umana e, per converso, dal modo di essere dell'intelligenza umana si desumono gli attributi che l'opera deve rivestire per poter aspirare alla tutela d'autore, ovvero per poter essere considerata un'opera dell'ingegno. Ma, a ben vedere, dietro la debolezza di questo ragionamento si cela qualcosa di più grave che attiene alla questione cui accennavo in precedenza e che investe lo spazio riservato al diritto

[10] Sul versante legislativo vanno ricordate la Direttiva 2009/24/CE (in materia di tutela del *software*); la Direttiva 96/9/CE (in materia di tutela delle banche dati); la Direttiva 2006/116/CE (in materia di durata della protezione del diritto d'autore e di alcuni diritti connessi). In particolare, con riguardo al *software* (considerando n. 7 e art. 1, co. 3 dir. *software*) e alle opere fotografiche (considerando n. 16 e art. 6 dir. durata), il legislatore eurounitario ha stabilito, in punto di originalità, che quest'ultima sussiste allorché l'opera sia il «risultato della creazione intellettuale dell'autore»; mentre con riguardo alle banche dati (considerando n. 16 e art.3, co.1 dir. banche dati) l'opera dovrà considerarsi originale allorché risulti essere una «creazione dell'ingegno propria del loro autore». A partire dalla sentenza Infopaq (Sentenza del 16 Luglio 2009, *Infopaq*, C-5/08, EU:C:2009:465), la Corte di Giustizia si è fatta carico di un'armonizzazione per così dire orizzontale, ovvero di portata generale, del requisito della originalità/creatività, prendendo le mosse dall'art. 2, lett. a) Direttiva 2001/29/CE (relativa all'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione: c.d. dir. Infosoc) a mente del quale «gli Stati membri riconoscono ai soggetti sotto elencati il diritto esclusivo di autorizzare o vietare la riproduzione diretta o indiretta, temporanea o permanente, in qualunque modo o forma, in tutto in parte». Orbene, ad avviso della Corte, poiché, come si ricava dai considerando nn. 4,9, 10, 11 e 20 della dir. Infosoc, quest'ultima, nell'istituire un quadro giuridico armonizzato, non può che basarsi sul medesimo principio accolto dalle dir. *software*, banche dati e durata secondo il quale, come si è visto, la tutela è subordinata alla circostanza che l'opera sia originale, cioè rappresenti il risultato della creazione intellettuale dell'autore, ne consegue che l'esclusiva in materia di diritto di riproduzione stabilita dal già richiamato art. 2, lett. a dir. Infosoc non può che applicarsi ad un oggetto che rivesta carattere di originalità, ossia, appunto, rappresenti il risultato dello sforzo creativo dell'autore (punti 35-37 della decisione Infopaq). Dati questi presupposti, dal momento che per quanto riguarda gli articoli di giornale (era questo il tipo di opera su cui verteva la controversia), il requisito dell'originalità risiede nelle modalità con cui è presentato il soggetto nonché dall'espressione linguistica, «non può escludersi che talune frasi isolate o, addirittura, talune parti di frasi del testo di cui trattasi, siano idonee a trasmettere al lettore l'originalità di una pubblicazione quale un articolo di giornale, comunicando a chi legge un elemento che è in se stesso espressione della creazione intellettuale dell'autore di tale articolo» (punti 44-47). Sicché anche un estratto di sole 11 parole che restituisca immediatamente ed efficacemente al lettore il senso dell'articolo indicizzato può integrare gli estremi di un'opera dell'ingegno. Insomma, la Corte di Giustizia, attraverso il medio dell'art. 2, lett. a) dir. Infosoc, assoggettato, invero, ad una lettura abbastanza stiracchiata, traghetta nel cielo dei concetti generali la nozione, davvero basica, di originalità approntata dal legislatore europeo con riferimento ad alcune specifiche tipologie di opere dell'ingegno ad alta densità tecnologica. Una nozione di originalità la quale, in definitiva, poggia sull'idea che il carattere creativo dell'opera discenda dall'esercizio, da parte dell'autore, della sua libertà di scelta quanto alla forma espressiva da imprimere all'artefatto. È abbastanza singolare che, istituita una soglia tanto bassa di originalità (tutta la giurisprudenza della Corte di Giustizia successiva ad Infopaq si muove in questa direzione, a cominciare dall'altrettanto celebre caso Painer (Sentenza del 1 December 2011, *Painer*, C-145/10, EU:C:2011:798) nel quale ad assicurare l'originalità dell'opera, una fotografia, è sufficiente la scelta dell'autore in quanto ad oggetto, angolatura, luce ecc. Per una disamina accurata degli orientamenti della Corte di Giustizia si rinvia a S. Guizzardi, *Il requisito della originalità delle opere dell'ingegno come armonizzato dalla Corte di Giustizia*, in *AIDA*, 2020, 3 ss.), se ne ricavi una insormontabile direttiva di ascrivibilità dell'opera dell'ingegno al solo *human being*: si v. così, ad es., A. Ramalho, *Originality redux*: *an analysis of the originality requirement in AI-generated works*, in *AIDA*, 2018, 23 ss. Analogo orientamento ha sposato il USA Copyright Office.

nell'economia della regolazione dei processi sociali. Lo statuto semantico del quesito relativo alla tutelabilità delle opere "create" dall'IA è di tipo descrittivo, non di tipo prescrittivo o deontologico: questo significa che il modo corretto di formulare la domanda è: "le opere "create" dall'IA sono opere dell'ingegno?" e non "le opere "create" dall'IA sono, in realtà, espressione della creatività umana?". In altre parole, se si vuole collocare nella giusta prospettiva il tema di cui ci stiamo occupando, è necessario, anche solo a mo' di ipotesi o di esperimento intellettuale, prendere in considerazione la possibilità di disembricare l'originalità dell'opera dalla sua matrice umana (salvo, poi, in una fase successiva dell'indagine, appurare che all'origine dell'opera "creata" dall'IA si trova pur sempre uno *human being*), spezzando, così, quel nesso tra "creativo" e "umano" dietro la cui fallacia sul piano logico si cela il delirio di onnipotenza del diritto.

Non so se ogni discorso sull'IA, ma certamente il discorso sull'IA e la sua regolamentazione giuridica dovrebbe muovere da un assunto, a mio avviso non contestabile: e cioè che l'IA porta alla luce una lacuna cognitiva del diritto e non, semplicemente, una lacuna assiologica. Intendo dire che il fenomeno dell'IA è radicalmente nuovo, introduce uno scarto tra la rappresentazione del mondo che sta dietro l'impresa giuridica e la realtà sulla quale quest'ultima esercita la sua pretesa regolatoria e, quindi, non può essere affrontato riproponendo, puramente e semplicemente l'insieme di regole e principi accumulatosi in costanza di un tempo nel quale parlare di creatività era lo stesso che parlare di creatività umana. Altrimenti, come ho già osservato, si converte indebitamente un problema di ordine ontologico in un problema di ordine deontologico: conversione di cui è un chiaro indice, sul piano logico – linguistico, la presunta inscindibilità del nesso creatività – *human being* la quale, viceversa, alla luce del nuovo mondo, si rivela fallace perché essa non può più essere presupposta (donde, appunto, la sua circolarità) ma esige, per la prima volta nella storia, di essere provata.

Il diritto, in altri termini, non è abilitato a dare una risposta negativa al quesito circa la tutelabilità delle opere dell'IA semplicemente perché non dispone (o dispone solo in apparenza) delle risorse necessarie per farlo. L'"artificiale" che, di per sé, non è una novità nella storia della specie, anzi ne identifica un tratto dominante, nelle sue declinazioni odierne, tuttavia, grazie ai vertiginosi progressi della tecnica, mostra la tendenza a sostituirsi, piuttosto che soltanto ad ausiliare, il suo *artifex*: certo, questa non è una buona ragione per abbandonarsi a chissà quali apocalittiche previsioni sul nostro futuro, ma neppure ci si può accontentare della rassicurante (ma anche un tantino ipocrita) esortazione rivolta dal maggiordomo alla sua padrona, la marchesa, mentre le fiamme di un incendio devastante divorano il castello avito. Di fronte ad un nuovo così radicale, il diritto non può trincerarsi dietro le vecchie certezze ma deve mettersi, piuttosto, alla ricerca di soluzioni ragionevoli, all'altezza di una transizione tanto profonda nei contenuti quanto incerta negli esiti[11].

[11] A proposito di "artificiale", un'analogia forse non del tutto peregrina può rintracciarsi nella fecondazione artificiale. Anche in quel caso eravamo al cospetto di una tecnologia della riproduzione che sostituiva quella "naturale": ma il "naturale" cessa di essere tale nel momento in cui viene affiancato dall' "artificiale" o, per lo meno, declassa a cognizione puramente descrittiva di una possibile (non più l'unica) modalità della riproduzione della specie: sicché, anche in quel caso, il richiamo alla "natura" quale strategia di fondazione di limiti e divieti assumeva una connotazione ideologica. Più complessa la faccenda diviene allorché la nuova

2. L'IA e gli *input*.

Una volta stabilito che l'appello allo *status quo* è, concettualmente, un fuor d'opera, il problema può essere riportato alla misura del diritto, in quanto sottosistema sociale erogatore di prestazioni specificamente rivolte alla soluzione di problemi pratici attraverso la tecnica dell'attribuzione di titoli giuridici. Questo ambiente è quello che più propriamente si addice alla spendita di argomenti pragmatici o, come dicevamo prima, orientati alle conseguenze[12]. Il discorso deve necessariamente prendere le mosse dalla circostanza che le opere "create" dall'IA possono rivestire, e in fatto, rivestono il carattere dell'originalità: si tratti di opere letterarie (articoli di giornale, saggi scientifici, racconti), di opere dell'arte figurativa (disegni, fotografie), di opere musicali (brani, selezione di brani) ecc. Di fronte a questo dato, contestabile solo al prezzo di ricadere nel circolo vizioso denunciato al § 1, e, peraltro, con effetti disastrosi dal punto di vista giuspolitico, le strategie da seguire sono fondamentalmente due: o ritenere che la vera artefice di queste opere sia pur sempre un'intelligenza umana (ad es., il programmatore), di talché avremmo messo in salvo l'infrastruttura di base della tutela autoriale (l'originalità dell'opera e il rintracciamento di un autore); ovvero, praticare fino in fondo la scissione tra l'opera e il suo artefice con la conseguenza che il problema non sarà più quello della individuazione di un autore nel senso tradizionale del termine, quanto, piuttosto, quello della individuazione di un soggetto al quale attribuire la titolarità dei diritti di utilizzazione economica dell'opera (ad es., l'utilizzatore del sistema, sulla falsariga della regola già sperimentata con riguardo alle banche dati non creative). Perché la vera posta in gioco è l'attrazione di quest'ultima nell'orbita del tutelabile, l'alternativa, disastrosa appunto, essendo costituita dalla sua caduta in pubblico dominio: disastrosa, in primo luogo, per quanti siano titolari di diritti sulle opere dell'ingegno a partire dalle quali l'IA ha "creato" il suo peculiare artefatto.

Il cuore della questione è rappresentato dal *training*, ossia dalla somministrazione ai dispositivi di IA evoluti, cioè congegnati per apprendere e per autocorreggersi (*machine learning*), di una enorme quantità di dati in una forma che ne consente il trattamento da parte del sistema con esiti che, a volte, non sempre e non necessariamente (si pensi al caso in cui il punto di approdo del processo sia una banca dati non creativa o una raccolta di metadati) mostrano i caratteri dell'opera dell'ingegno. Dal punto di vista del diritto d'autore, il *training* è una spina nel fianco perché i dati sulla base dei quali i sistemi di IA apprendono e poi elaborano l'*output*, cioè il risultato finale visibile all'utilizzatore sono spesso costituiti da opere dell'ingegno non ancora cadute in pubblico dominio. Qui fa capolino un vero paradosso: il ripudio, di tutto principio, della possibilità che quelle confezionate dall'IA generativa siano opere dell'ingegno apre un varco temporale – una sorta di pubblico dominio anticipato – dentro il quale vengono risucchiate tutte le opere "prime"

tecnologia viene posta al servizio di modalità riproduttive che incidono direttamente sul legame sociale, ovvero quando l'"artificiale" è strumento di riscrittura di codici culturali consolidati la difesa, o il superamento dei quali, legittimamente impegnano il diritto ad una presa di posizione che può essere anche di ripulsa: emblematica, al riguardo, la vicenda della maternità surrogata nelle sue varie forme.

[12] V., al riguardo, le pertinenti osservazioni di S. GUIZZARDI, *La protezione d'autore dell'opera dell'ingegno creata dall'intelligenza artificiale*, in *AIDA*, 2018, 42 ss.

utilizzate per il *training* della macchina. In altre parole, la difesa ad oltranza dell'anima antropocentrica del diritto d'autore crea le premesse per una sua crisi, probabilmente fatale là dove viene minata, *obliqua via*, l'effettività di uno dei baluardi su cui esso storicamente si è fondato: cioè, il controllo riservato all'autore sulle rielaborazioni creative dell'opera il quale, però, può essere invocato solo se l'opera a valle gode della protezione legale. Per converso, è anche vero che, come viene fatto osservare da quanti si affidano, per contrastare l'ingresso degli artefatti generati dall'IA nel *sancta sanctorum* delle opere dell'ingegno, ad un argomento di tipo pragmatico e non solo di tipo ideologico (inconsistente, come si è visto), la prodigiosa capacità riproduttiva di questi sistemi rischia di portare la creatività al collasso, saturando il mercato di opere dell'ingegno "seriali" (nella produzione, non nei contenuti) e, dunque, disincentivando lo sforzo creativo degli autori umani. Il paradosso, dunque, finisce per vestire i panni del dilemma: o penalizzare le opere che alimentano il *training* dei sistemi di *machine learning*, quindi la creatività passata, o scoraggiare la creatività futura, imponendole la missione impossibile di competere con la serialità delle macchine.

3. L'IA e gli *output*.

Un altro pilastro del nostro edificio che l'IA generativa mette, se non in crisi, almeno in discussione è l'antitesi idea – forma espressiva. La tutela d'autore muove da un assunto abbastanza elementare, e cioè che la nostra specie, per quanto riccamente dotata rispetto alle altre specie animali che popolano il pianeta, alla fine, più o meno, si ripete. Se, per avventura, l'opera dell'ingegno coincidesse con il suo tema ispiratore, dopo l'Iliade e l'Odissea sarebbe stato veramente difficile scrivere qualcosa di originale. Abbiamo un'opinione molto elevata di noi stessi ma, alla fine, facciamo più o meno sempre le stesse cose: la guerra (attività alla quale ci dedichiamo con grande zelo e profusione di nobili motivazioni), la ricerca del potere e del denaro, l'amore, nelle sue varie declinazioni, l'affermazione personale, il cibo, l'alcool e pochissimo altro. Quindi, ad essere tutelato non è il tema ma la sua variazione: appunto, non l'idea ma il modo in cui viene espressa attraverso le forme della cultura e il sistema di segni al quale ciascuna di queste forme si affida (la letteratura, le arti figurative, la cinematografia ecc.).

Nel mondo di ieri questa intelaiatura funzionava piuttosto bene. In definitiva, la distinzione tra l'idea (non protetta) e la sua espressione artistica (protetta) permetteva di istituire una prima linea di difesa, tanto rudimentale quanto efficace, incardinata sul monopolio della riproduzione, quello che potremmo considerare il protodiritto di utilizzazione economica, a beneficio dell'autore. Certo, l'avvento e la diffusione delle tecnologie digitali, mettendo tutti nelle condizioni di copiare *ad libitum* e per di più a costo zero, hanno reso necessario un rafforzamento dell'esclusiva sulla riproduzione, estendendone molecolarmente il campo applicativo (basti pensare agli artt. 2 e 5 della Direttiva Infosoc del 2001): ma è altrettanto vero che una copia è pur sempre una copia, per quanto agevole sia realizzarla sicché, restando i limiti del tutelabile saldamente presidiati da un addentellato nella realtà fisica (la copia,

appunto), anche la distinzione tra idea e forma espressiva mantiene la sua originaria ragion d'essere.

Nel mondo di oggi, e, verosimilmente, ancora di più nel mondo di domani, qualche dubbio, sulla tenuta di quella distinzione, è e sarà lecito nutrirlo. Proprio l'avvento dei sistemi di IA i quali vengono istruiti attraverso la somministrazione di un numero impressionante di dati sulla base dei quali, attraverso un percorso di apprendimento e di autocorrezione, la macchina, opportunamente stimolata, è in grado di restituire un *output* (si tratti di un disegno, di una fotografia, di un racconto) che non è una copia dell'originale (anche perché, appunto, gli *input* sui quali viene svolto il t*raining* sono in genere numerosissimi) ma non è neppure una rielaborazione creativa in senso proprio, del tipo di quelle note al diritto d'autore tradizionale (adattamenti cinematografici, traduzioni ecc.) perché il legame con l'originale si è allentato sino al punto da condividere con quest'ultimo soltanto un'aria di famiglia, un tratto, riconoscibile, ma pur sempre un semplice tratto, uno stile.

Si dirà che, in definitiva, opere "alla maniera di" ci sono sempre state e che ogni grande artista può contare sul suo drappello, più o meno nutrito, non solo di imitatori ma anche di adepti i quali si ispirano alle sue opere e al suo stile per assecondare e coltivare la loro spinta creativa. E, del resto, è opinione comune che lo stile, la maniera, appunto, per quanto inconfondibili, non possono essere fatti rientrare nella sfera protetta dal *copyright*, pena l'estensione di quest'ultima ben al di là di quanto richiesto dagli obiettivi tradizionalmente perseguiti dalla tutela d'autore. Non si può trascurare, però, la circostanza che con i sistemi di IA la riproduzione dello stile assume un carattere seriale e che attraverso l'impiego di processi sempre più sofisticati la distanza dall'originale tende ad accorciarsi senza che per questo si possa parlare di copia. Insomma, nelle mani dell'IA, il binomio idea/forma espressiva si opacizza, nel senso che perde quel tratto di affidabilità che ne ha fatto, da sempre, un dispositivo linguistico a partire dal quale impiantare il discorso sulla tutela d'autore.

4. IA e proprietà intellettuale: molto più che una semplice lesione.

Naturalmente può ben accadere che attraverso questi programmi di apprendimento e autocorrezione il diritto di riproduzione venga violato. Evenienze simili si danno allorché i dati somministrati all'IA, invece che essere disaggregati e poi ricomposti (*non expressive use*), vengano memorizzati e restituiti all'utilizzatore finale nella loro configurazione originaria (*memorization*)[13]. Ciò, in particolare, può verificarsi quando l'*output* riproduce un testo o un disegno che nel corso della fase di *training* siano "passati" più di una volta in tal modo agevolando, per l'appunto, la memorizzazione del modello e, conseguentemente, la sua riproduzione in linea di massima fedele. Tuttavia, non mi sembra che fenomeni di questo genere, di patente *infringement* della proprietà intellettuale, rappresentino il cuore del problema: e, per la verità, un modo sicuro di trasformare una questione piuttosto banale in un problema è, appunto, quello di negare agli *output* dell'IA la dignità di

[13] M. Sag, *Copyright Safety for generative AI*, in *Forthcoming in Houston Law Review*, 2023, II, 61 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4438593.

opere dell'ingegno consegnandoli al territorio, in questo caso per nulla ospitale, del pubblico dominio.

Arrivati a questo punto, alla luce delle brevi osservazioni svolte sin qui, vorrei dire qualcosa a proposito del titolo di questa relazione, "IA e lesione della proprietà intellettuale": un titolo che a me pare un tantino ingannevole, per i motivi che vedremo subito. La storia della proprietà intellettuale e, per quello che più da vicino ci interessa, la storia del diritto d'autore, è una storia di crisi e correlativi adattamenti di vario tipo, in primo luogo di tipo legislativo. Queste crisi, strettamente collegate, in primo luogo, all'evoluzione della tecnologia ma anche all'influenza che il progresso delle conoscenze esercita sul pensiero in generale, e sul modo di intendere l'arte in particolare, assumono, in definitiva, due posture basilari. In un primo caso, infatti, si assiste ad un attacco diretto alle prerogative riconosciute all'autore: dalla contraffazione alla reprografia sino all'avvento delle tecnologie digitali e poi della rete, il nucleo essenziale del fascio di diritti di cui si compone l'esclusiva è stato costantemente insidiato, e negli ultimi decenni con intensità crescente, inducendo il legislatore (nazionale, sovranazionale, internazionale) ad adottare misure ora di ipertrofico rafforzamento dell'esclusiva medesima (il caso del diritto di riproduzione, già ricordato, è emblematico), ora di retribuzione dello sforzo creativo di tipo forfettario (l'equo compenso).

Nel secondo caso, viceversa, la crisi si insedia nel cuore stesso del diritto d'autore inteso, ancora prima che come strumento di regolazione di certi fenomeni, come dispositivo deputato alla trascrizione nel linguaggio del diritto di quegli stessi fenomeni. In altre parole, ad entrare in crisi è non solo, o non tanto, l'effettività del *copyright*, quanto piuttosto la sua attitudine cognitiva: e ciò si verifica tutte le volte in cui esso venga scavalcato da un particolare modo di atteggiarsi dell'intreccio di tecnica, pensiero artistico e forme espressive che ne mettano in crisi le categorie di lettura del reale provocandone un radicale disorientamento[14]. È già accaduto, per citare un precedente illustre, con l'arte concettuale; ed è quello che sta accadendo con l'IA e la sua inedita capacità di confezionare opere che, attraverso la scomposizione e la ricomposizione dei *latent features* caratterizzanti uno stile, si dislocano, come abbiamo visto, esattamente a cavaliere di idea e forma espressiva. Ecco perché a me sembra che l'IA metta in discussione, dalle fondamenta, l'edificio del diritto d'autore; ed ecco anche la ragione per la quale, a mio avviso, il titolo della relazione è un po'fuorviante: perché, in realtà, ciò che l'IA fa alla proprietà intellettuale è molto più che lederla nel senso tradizionale del termine, la scompagina letteralmente e costringe ad un suo radicale ripensamento. Uno sviluppo come l'IA, con le caratteristiche che abbiamo richiamato per sommi capi, non si lascia imbrigliare all'interno di manovre asfittiche di aggiustamento delle coordinate di fondo del *copyright*, perché sono queste ultime ad essere in crisi.

[14] Sul punto v. G. Ajani, *Contemporary Artificial Art and Law. Searching for an Author*, in *Art & Law*, 2019, 1 ss.

5. "Produzione di opere dell'ingegno per mezzo di opere dell'ingegno": dalla tutela d'autore al diritto dei contratti.

Vi è un punto intorno al quale si registra un sostanziale consenso che accomuna coloro i quali, non riuscendo ad accettare l'idea che la creatività possa divorziare dall'umano, negano alle opere dell'IA la dignità di opere dell'ingegno, a coloro i quali, viceversa, si orientano nella direzione esattamente opposta e così rinvengono negli *output* dell'IA il carattere dell'originalità: e cioè che, almeno allo stadio attuale della sviluppo tecnologico, l'IA non è in grado di fare tutto da sola, ma necessita, per l'appunto, di un *input* e dell'apprendimento di un linguaggio che le permetta di elaborare, anche attingendo un elevato grado di autonomia, quegli *input*. Bisogna guardarsi, però, da un uso corrivo di questo argomento: a nessuno verrebbe in mente di negare dignità di opera dell'ingegno ad uno scritto munito del grado di originalità necessario e sufficiente (molto basso, come si è visto) solo perché il linguaggio nel quale è stato composto è quello appreso dall'autore alla scuola elementare; e neppure di arrivare alla medesima conclusione solo perché lo scritto in questione intercetta e rielabora, in modo originale, materiale, stile, tradizione culturale rinvenibile nell'ambiente in cui l'autore è immerso. Si potrebbe dire, semmai, che qui la realizzazione dell'opera costituisce l'oggetto di una scelta, attuata dall'utilizzatore: una scelta che non soltanto non si identifica con quelle che culmineranno nell'allestimento dell'*output*, ma che, per di più, fa capo ad un soggetto – uso il termine nell'accezione più lata e atecnica possibile – diverso da quello che si farà carico dell'allestimento medesimo. In altre parole, si assiste, nel caso delle opere generate dall'IA, ad una scissione del processo creativo: la decisione di confezionare l'opera, ancora nella piena disponibilità dell'umano, le scelte che conducono alla elaborazione dell'opera, ormai affidate alla macchina. Questa scissione non soltanto rende difficile stabilire con esattezza l'incidenza dell'uno e dell'altro rapporto[15], ma finisce per imprimere all'opera dell'ingegno una fisionomia del tutto inedita e, ancora una volta, difficilmente riconducibile alle architetture della tutela d'autore tradizionalmente intesa.

Il ruolo preponderante che l'artificiale occupa oggi nella produzione dell'opera dell'ingegno ha come corollario quello di rendere artificiale anche il *fiat* che sta all'origine di quel processo. Da questo punto di vista, mi sembra di poter ravvisare una non banale analogia con le trasformazioni subite dall'economia inglese durante il XVIII secolo, nel passaggio dal laboratorio domestico alla filanda e, poi, alla fabbrica: insomma, la Rivoluzione industriale. Il fenomeno di cui oggi siamo testimoni – fenomeno destinato a dilatarsi nei prossimi anni – è quello, per parafrasare Sraffa, della produzione di opere dell'ingegno (*output*) per mezzo di opere dell'ingegno (*input*), con la conseguente nascita di un nuovo mercato – il mercato delle opere dell'ingegno create dall'IA – il quale, come tutti i mercati, impone di andare alla ricerca di una soluzione regolatoria che, nel nostro caso, vuol dire andare definitivamente oltre il paradigma romantico che sta a fondamento della tutela d'autore, specie di quella di ispirazione eurocontinentale, per abbracciare, senza esitazioni la

[15] G. Rossi, *L'intelligenza artificiale e la definizione di "opera dell'ingegno"*, in *AIDA*, 2018, 268 ss.

prospettiva che vede in ciò a cui stiamo assistendo un processo industriale, catturabile dal diritto solo attraverso un approccio integrato.

L'analogia con la Rivoluzione industriale e con la trasformazione in senso capitalistico dell'economia risulta, da questo punto di vista, particolarmente calzante. Gli *input* – opere dell'ingegno nella generalità dei casi ancora tutelate – rappresentano un valore d'uso per procurarsi il quale l'utilizzatore deve pagare un corrispettivo. Naturalmente, è impensabile che queste transazioni possano avvenire su base individuale, vuoi perché i costi lieviterebbero in modo spropositato, vuoi perché per il singolo autore tracciare le proprie opere somministrate per il *training* dell'IA sarebbe praticamente impossibile. Si può pensare a forme di negoziazione affidate a *collecting society*, a carattere forfettario e agganciate alla quantità di *output* immessi sul mercato da ciascun singolo utilizzatore, oltreché al fatturato realizzato: un modello chiaramente ispirato alle società di gestione collettiva e all'equo compenso tipici del *copyright*, ma con una differenza cruciale, che dovrebbe risultare chiara alla luce di quanto osservato al § 3, e cioè che qui a fondare la remunerazione non è l'esclusiva sulla riproduzione/rielaborazione dell'opera dell'ingegno, ma appunto il suo venire in considerazione come valore d'uso per l'utilizzatore e, conseguentemente, come valore di scambio per l'autore. Dalla disciplina generale in materia di diritto d'autore si potrebbero mutuare anche gli obblighi di informazione ora previsti dall'art. 110 - *quate*r l. dir.aut.: obblighi, dunque, intesi a rendere edotti gli autori, per il tramite dei loro organismi di gestione collettiva, delle attività svolte e dei ricavi realizzati dall'utilizzatore.

Insomma, a mio avviso, ma si tratta di un'opinione già abbastanza diffusa in dottrina, il fenomeno va riguardato nella prospettiva del diritto dei contratti piuttosto che in quella della tutela d'autore: il ruolo di questa è destinato ad essere marginale, ovvero confinato alle ipotesi di plateale *infringement* da parte dell'utilizzatore. Quest'ultimo, dal canto suo, dovrà reputarsi il titolare dei diritti di utilizzazione economica sull'opera creata dall'IA: e nel mercato a valle, dove l'opera dell'ingegno, ossia l'*output*, viene in considerazione immediatamente come valore di scambio, le regole del copyright potranno tornare ad applicarsi, almeno di *default*.

Achille D, 'I «Registri delle attività di trattamento» tra responsabilizzazione e presupposto di liceità del trattamento dei dati personali' (2024) 2 EJPLT, 102 – 114.
DOI: https://doi.org/10.57230/EJPLT242DA

EJPLT
ISSN 2704-8012



I «Registri delle attività di trattamento» tra responsabilizzazione e presupposto di liceità del trattamento dei dati personali

«Records of processing activities» between accountability and the prerequisite of lawfulness of personal data processing

DAVIDE ACHILLE
Professore Associato di Diritto Privato
Università del Piemonte Orientale

Abstract

Il GDPR ha previsto l'obbligo di tenuta dei registri delle attività di trattamento quale strumento di concretizzazione del principio di responsabilizzazione (c.d. accountability) cui è improntata la normativa europea sulla protezione dei dati. Attraverso l'analisi della normativa di riferimento e mediante l'individuazione della disciplina applicabile ai registri delle attività di trattamento, si rileva come questi svolgano altresì la funzione di consentire la valutazione e la documentazione della conformità del trattamento al GDPR esplicitando quel necessario bilanciamento tra diritto all'informazione e diritto alla riservatezza che sottende alla normativa sulla tutela dei dati personali.

The GDPR has provided for the obligation to keep records of processing activities as a tool for implementing the principle of responsibility (so-called accountability) to which the European data protection legislation is guided. Through the analysis of the relevant legislation and through the identification of the discipline applicable to the records of processing activities, it is noted how they also perform the function of enabling the evaluation and documentation of the compliance of processing with the GDPR by making explicit that necessary balance between the right to information and the right to confidentiality that underlies the legislation on the protection of personal data.

* Il presente contributo è destinato allo special issue in memoria del Prof. Cesare Massimo Bianca e del Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy» da lui curato con il Prof. Francesco Donato Busnelli nel 2007 (Cedam).

© The author(s) 2024, 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: dati personali; trattamento; registro delle attività; accountability

Summary: 1. I registri dell'attività di trattamento e la responsabilizzazione. – 2. Il registro del titolare del trattamento. – 3. Il registro del responsabile del trattamento. – 4. Le regole di tenuta e di gestione dei registri. – 5. L'obbligo di mettere a disposizione del Garante il registro. – 6. Le esenzioni. – 7. I registri come strumenti di valutazione e documentazione della conformità del trattamento al GDPR.

1. I registri dell'attività di trattamento e la responsabilizzazione.

Nell'insieme delle varie novità apportate dalla normativa europea in tema di protezioni dei dati personali (Regolamento (UE) 2016/679 [1]) si inserisce senz'altro la previsione dell'obbligo di tenuta del registro dell'attività di trattamento[2] che, secondo l'art. 30 *GDPR*, costituisce un incombente a carico del titolare del trattamento, del responsabile del trattamento e, ove presente, del loro rappresentante[3], siano questi soggetti pubblici o privati. In particolare, viene prevista la tenuta di due differenti registri dell'attività di trattamento, quello del titolare del trattamento[4] e quello del responsabile del trattamento[5], comminando per la relativa omissione specifiche sanzioni[6].

[1] Per una visione d'insieme sul GDPR, oltre alle opere citate nel prosieguo, v. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016; G. Busia-L. Liguori-O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, 2016; L. Califano-C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/ 679*, Napoli, 2017; V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy)*, Milano, 2019; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati: riflessioni sul GDPR*, Padova, 2019.

[2] Sul tema, per una prima informazione, v. L. Bolognini, *Obbligo di documentazione*, in L. Bolognini-E. Pelino-C. Bistolfi, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 413 ss.

[3] Con riferimento al concetto di rappresentante rilevante ai fini del discorso che ci occupa, v. S. Melchionna, *Art. 30*, in *GDPR e normativa privacy* a cura di G.M. Riccio-G. Scorza-E. Belisario, Vicenza, 2018, p. 284, la quale ritiene «utile riferirsi alla copiosa giurisprudenza del GPDP sul tema e ad alcune disposizioni già presenti nel CPDP che richiamano espressamente le attività sulle quali il titolare esercita un potere decisionale su finalità e mezzi con conseguente responsabilità».

[4] Il titolare del trattamento è definito dall'art. 4, n. 7, *GDPR*, come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

[5] Il responsabile del trattamento è definito dall'art. 4, n. 8, *GDPR*, come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

[6] La mancata tenuta dei registri viene sanzionata, ai sensi dell'art. 83, par. 4, lett. a), *GDPR*, con una pena pecuniaria fino a 10.000.000 di euro o, per le imprese, fino al 2% del fatturato dell'esercizio precedente, se superiore. Rileva inoltre S. Melchionna, *op. cit.*, p. 291, che l'inadempimento all'obbligo di tenuta dei registri «può essere considerato dal GPDP come elemento valutativo nell'ambito dell'esercizio dei propri poteri di intervento e controllo».

Al di là delle non trascurabili implicazioni che tale adempimento comporta a livello di *compliance* aziendale rispetto alla normativa di riferimento[7], la tenuta del registro in questione costituisce una delle misure in cui si estrinseca con maggiore evidenza il principio di responsabilizzazione (c.d. *accountability*) di cui all'art. 5, par. 2, *GDPR*[8]. Infatti, come si evince dal Considerando n. 82, «per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità».

A tal ultimo riguardo, sulla base del rilievo per cui la responsabilizzazione deve consistere anche in una serie di attività che consentano di comprovare il rispetto delle norme contenute nel *GDPR* e l'adozione di misure efficaci, è stato opportunamente rilevato che la tenuta del registro delle attività di trattamento, piuttosto che costituire un mero adempimento formale, è «parte integrante di un approccio sostanziale alla tutela dei dati e delle persone nell'ambito di un sistema di corretta gestione dei dati personali»[9].

In questo contesto, per quanto la tenuta dei registi delle attività di trattamento si ponga in continuità con l'obbligo di notificazione di cui agli artt. 37 s., d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali)[10], oggi abrogato dall'art. 27 del d.lgs. 10 agosto 2018, n. 101, si distingue profondamente dal previgente incombente in quanto non integra il dovere di comunicare all'autorità competente lo svolgimento di determinati trattamenti, costituendo invece uno «strumento di ricognizione delle attività svolte[11], che si colloca in un sistema trasparente di corretta gestione dei dati

[7] È infatti innegabile che l'adempimento dell'obbligo di tenuta dei registri dell'attività di trattamento ha costituito e costituisce un incombente particolarmente gravoso, specialmente per quelle grandi realtà in cui l'ordinaria attività imprenditoriale implica per sua natura il trattamento di una innumerevole quantità di dati personali (si pensi, ad es., alle aziende di telecomunicazione e agli istituti di credito). L'affermazione non deve tuttavia essere enfatizzata, dovendosi riconosce che la predisposizione dei registri in parola risulta in concreto facilitata dagli obblighi previsti dalla normativa previgente, la quale già prevedeva la tenuta del documento programmatico sulla sicurezza (D.P.S.) di cui all'Allegato B (Disciplinare tecnico in materia di misure minime di sicurezza) del d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), oggi abrogato dall'art. 27, co. 1, lett. d), del d. lgs. 10 agosto 2018, n. 101, il cui contenuto era individuato dal punto 19 del citato Disciplinare tecnico in materia di misure minime di sicurezza. Può quindi ritenersi che, pur a fronte della differente logica sottesa ai due adempimenti (CONTI, *La tenuta dei registri: consapevolezza,* accountability, substance over form *e documentazione delle scelte*, in *Foro padano*, 2019, c. 42), la nuova previsione che impone la tenuta del registro delle attività di trattamento non sia totalmente inedita (L. GIACOMINI-C.A. TROVATO-C. ROSSI CHAUVENET, *Il registro delle attività di trattamento previsto dal GDPR: più di uno strumento di mera* compliance, in *MediaLaws*, 2018, p. 461).

[8] Sul ruolo del principio di responsabilizzazione nel quadro del *GDPR,* v. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Leggi civ. comm.*, 2017, 1 ss.; ID., *Il principio di* accountability, in *Giur. it.*, 2019, p. 2778 ss.

[9] Cfr. MELCHIONNA, *op. cit.*, p. 283.

[10] Al riguardo, v. R. ROSETTI, *Artt. 37-38*, in *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)* a cura di C.M. BIANCA e F.D. BUSNELLI, I, Padova, 2007, p. 732 ss.

[11] Sul punto v. anche la Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali emanata dal Garante per la protezione dei dati personali (doc. web. n. 6807118), disponibile all'indirizzo *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6807118*, dove si rileva che nella nuova prospettiva del *GDPR* l'intervento delle autorità di controllo sarà principalmente *ex post*, ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiegando l'abolizione per effetto del d.lgs. 10 agosto 2018, n. 101 di alcuni istituti previsti dalla Direttiva 95/46/CE e dal d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior-checking* (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare e del responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia con eventuale

personali»[12]. È quindi corretto individuare l'obbligo di tenuta dei registri alla stregua di un adempimento prodromico ad ogni attività di trattamento dei dati personali in quanto funzionale a valutarne i rischi[13], costituendo quindi un prerequisito del trattamento stesso[14].

Ciò consente, inoltre, di ritenere che la tenuta dei registri in questione sia un obbligo per il titolare e per il responsabile, non potendo lo stesso essere demandato ad altro e diverso soggetto e, in particolare, al *data protection officer* (*DPO*)[15], posto che quest'ultimo è piuttosto tenuto a sorvegliare l'osservanza della normativa di riferimento da parte del titolare e del responsabile del trattamento (art. 39, par. 1 lett. b), *GDPR*), compito questo che riguarda quindi anche l'obbligo di tenuta dei registri in questione, con la conseguenza che onerando tale soggetto della tenuta dei registri in esame si realizzerebbe una inammissibile commistione tra controllore e controllato in evidente contrasto con i principi sottesi alla normativa europea in tema di protezione dei dati personali.

2. Il registro del titolare del trattamento.

Nel prevedere l'obbligo di tenuta del registro dell'attività di trattamento da parte del titolare[16], il par. 1 dell'art. 30 *GDPR* individua il contenuto, minimo ed essenziale, dello stesso. In particolare, si prevede che questo debba contenere: a) le indicazioni per l'individuazione del titolare, o contitolare, del rappresentante del titolare e del responsabile della protezione dei dati, comprensive dei relativi dati di contatto; b) l'indicazione delle finalità del trattamento; c) le categorie di interessati e di dati personali che vengono trattati; d) l'indicazione delle categorie di destinatari a cui i dati personali trattati possono essere comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, compresa l'identificazione del paese terzo o dell'organizzazione e, per i trasferimenti *ex* art. 49, par. 2, *GDPR*, la documentazione delle garanzie adeguate; f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) la descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 31, par. 1, *GDPR* che

successiva consultazione dell'Autorità, tranne che per alcune specifiche situazioni di trattamento (v. art. 36, par. 5, *GDPR*).

[12] M. SOFFIENTINI, *Registro dei trattamenti e dei data breaches*, in *Dir. e prat. lav.*, 2019, p. 1733.

[13] S. MELCHIONNA, *op. cit.*, p. 283 s., la quale rileva altresì il ruolo, riteniamo anche promozionale, di «un nuovo approccio culturale e organizzativo al trattamento».

[14] V. W. KOTSCHY, *Article 30. Records of processing activities*, in *The EU General Data Protection Regulation (GDPR). A Commentary* edited by C. Kuner-L.A. Bygrave-C. Docksey, Oxford, 2020, p. 618, dove si afferma che «Knowing which data are processed about what kind of data subjects and for what purpose is a prerequisite for being able to be held accountable».

[15] In questo senso, invece, A. AVITABILE, *Il* data protection officer, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* opera diretta da G. Finocchiaro, Bologna, 2017, p. 364, secondo il quale ciò sarebbe possibile in quanto il legislatore ha previsto una «elencazione non esaustiva dei compiti attribuibili al DPO», potendosi al riguardo rilevare che ciò non esclude che le competenze di tale soggetto siano determinate coerentemente con il ruolo allo stesso attribuito dal legislatore.

[16] Si è peraltro ritenuto che «laddove l'attività sia effettuata da più titolari in contitolarità, non solo la stessa sia censita nei registri di tutti i titolari, ma anche che ogni contitolare indichi con riferimento a quali trattamenti sussiste la contitolarità e con quali soggetti» (così S. MELCHIONNA, *op. cit.*, p. 285).

sono adottate con riferimento alle attività di trattamento.

Il contenuto eterogeneo cui fa riferimento la norma può essere suddiviso in due distinte categorie di informazioni che il registro deve avere, consentendo di distinguere tra profili prettamente afferenti al titolare del trattamento (contenuto formale) e aspetti riferibili ai dati che sono trattati (contenuto sostanziale).

Quanto al contenuto formale, oltre al riferimento al titolare, contitolare e responsabile, comprensivo delle relative informazioni per consentire una più agevole contatto con tali soggetti[17], devono essere indicate le categorie di destinatari a cui i dati possono essere comunicati [18] e, secondo quanto suggerito dal Garante per la protezione dei dati personali, anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento – siano trasmessi i dati da parte del titolare, al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali[19]. Quanto alle informazioni circa i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese terzo cui i dati sono trasferiti e alle adeguate garanzie adottate ai sensi degli artt. 44 ss. *GDPR*[20]. Infine, per quanto attiene la descrizione generale delle misure di sicurezza andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 *GDPR*[21], che si è ritenuto possano «essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale»[22].

Il contenuto sostanziale riguarda invece una serie di indicazioni direttamente riconducibili ai dati trattati. In primo luogo, occorre indicare il contenuto delle finalità del trattamento, con ciò intendendosi la base giuridica del trattamento[23], con la precisazione che in caso di trattamenti di categorie

[17] Cogliendo il parallelismo con il contenuto essenziale dell'informativa ai sensi dell'art. 13, par. 1, lett. a), *GDPR*, si è ritenuto che debbano essere indicati l'indirizzo, anche di posta elettronica certificata, il numero di telefono e di *fax* (S. MELCHIONNA, *op. cit.*, p. 280).

[18] Il destinatario, secondo quanto previsto dall'art. 4, n. 9, *GDPR* è «la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento».

[19] In questo senso le FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali (consultabili all'indirizzo *www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*).

[20] Con riguardo all'indicazione delle «garanzie adeguate», ci si è chiesti se debbano essere allegati i documenti a supporto della legittimità del trattamento o sia sufficiente la mera indicazione delle garanzie adottate, ritenendo condivisibilmente che «la norma si riferisca esclusivamente alle informazione atte a provare tale adeguatezza e non specificatamente alla documentazione richiesta a tal fine» (L. GIACOMINI-C.A. TROVATO-C. ROSSI CHAUVENET, *op. cit.*, p. 456).

[21] S. MELCHIONNA, *op. cit.*, p. 288, secondo la quale, tramite la descrizione delle misure di sicurezza e l'analisi che vi sottende, «il registro si pone […] anche come strumento di pianificazione e controllo della politica di sicurezza».

[22] V. le FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali cui si è già fatto riferimento.

[23] Rileva S. MELCHIONNA, *op. cit.*, p. 286, che con riguardo ai soggetti pubblici «l'indicazione della finalità di trattamento implica una ricognizione delle disposizioni normative di settore, che attribuiscono al soggetto

particolari di dati occorre individuare la specifica condizione di cui all'art. 9, par. 2, *GDPR* e in caso di trattamenti di dati relativi a condanne penali e reati si deve indicare la specifica normativa che ne autorizza il trattamento ai sensi dell'art. 10 *GDPR*[24]. In merito alla descrizione delle categorie di interessati e di dati personali trattati, andranno specificate sia le tipologie di interessati, evidenziando se il trattamento riguarda particolari categorie di soggetti[25], sia le tipologie di dati personali oggetto di trattamento. Circa i termini ultimi previsti per la cancellazione delle diverse categorie di dati dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento e, dove non sia possibile stabilire a priori un termine massimo[26], i tempi di conservazione dovranno essere specificati mediante il riferimento a criteri indicativi degli stessi, tenendo in ogni caso presente che tale profilo deve essere necessariamente coordinato con il principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), *GDPR*, il quale impone che i dati siano conservati per un tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono trattati.

A fronte delle indicazioni circa il contenuto del registro del titolare che fornisce l'art. 30 *GDPR*, che – come detto – costituisce il contenuto minimo e essenziale del registro, è stato correttamente rilevata l'opportunità di un contenuto ulteriore del documento in parola, da implementare con ogni ulteriore informazione che si rendesse necessaria in base ad una valutazione complessiva di impatto della normativa applicabile rispetto ai trattamenti di dati in concreto effettuati[27]. La precisazione si giustifica, ed in ciò deve trovare conferma, sul rilievo che la tenuta del registro è funzionale al corretto e puntuale rispetto della regolamentazione in tema di protezione dei dati personali, in ottemperanza al principio di responsabilizzazione, il quale nella variabilità e nelle eterogeneità del caso concreto impone di adoperarsi per la miglior tutela dell'interessato e del sistema di protezione dei dati.

---

pubblico la specifica finalità per il raggiungimento della quale diviene indispensabile trattare i dati personali».

[24] Il chiarimento si trova nelle FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali cui si è già richiamato.

[25] V. S. MELCHIONNA, *op. loc. cit.*, la quale, in particolare, si riferisce a «minori, lavoratori, sottoposti a misure di privazione della libertà, rifugiati, beneficiari di provvidenze, disabili, pazienti, ovvero individui distinguibili per credo, convinzioni politiche o etnie».

[26] Si tengano presenti al riguardo le determinazioni specifiche di conservazione massima delle informazioni personali, come ad esempio previsto per la videosorveglianza comunale dall'art. 6, co. 8, d. l. n. 11 del 23 febbraio 2009, convertito in legge con modificazioni, dall'art. 1, co. 1, l. n. 39 del 23 aprile 2009, ai sensi del quale «La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione».

[27] V. S. MELCHIONNA, *op. cit.*, p. 288, che con riferimento al contenuto ulteriore indica la data di inizio del trattamento, la necessità di acquisire il consenso dell'interessato con riferimento ad una specifica attività di trattamento, l'indicazione di un accordo con il contitolare in ordine alle responsabilità sugli obblighi e sull'esercizio dei diritti, le informazioni circa il luogo dove risiedono i dati, le categorie di persone autorizzare al trattamento, l'adesione/adozione di codici di condotta, l'applicazione di meccanismi di certificazione, la sussistenza di una valutazione di impatto *privacy*, l'eventuale consultazione preventiva del Garante per la protezione dei dati personali, il verificarsi di un *data breach*.

3. Il registro del responsabile del trattamento.

Il contenuto del registro delle attività del responsabile del trattamento è individuato dal par. 2 dell'art. 30 *GDPR*, il quale riproduce in gran parte, con una tecnica normativa quantomeno discutibile, l'elencazione del contenuto del registro delle attività di trattamento del titolare previsto dal precedente par. 1 della medesima disposizione[28]. In particolare – oltre alle indicazioni necessarie per l'individuazione dei soggetti coinvolti nel trattamento (responsabile, titolare, rappresentante del titolare o responsabile del trattamento e responsabile della protezione dei dati), i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, compresa l'identificazione del paese terzo o dell'organizzazione e, per i trasferimenti *ex* art. 49, par. 2, *GDPR*, la documentazione delle garanzie adeguate e la descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 31, par. 1, *GDPR* che sono adottate con riferimento alle attività di trattamento – il contenuto peculiare che caratterizza il registro in parola è unicamente quello delle «categorie di trattamenti effettuati per conto di ogni titolare del trattamento». A differenza del registro tenuto dal titolare del trattamento, quello del responsabile non contiene invece l'indicazione del termine di cancellazione dei dati personali e l'indicazione delle finalità del trattamento, il che si spiega in ragione del diverso ruolo attribuito al responsabile rispetto al titolare del trattamento.

Ciò posto, anche per il registro del responsabile del trattamento come per quello del titolare, si deve ammettere la possibilità di implementare il contenuto del registro delle attività di trattamento prevedendo ulteriori indicazioni rispetto a quelle cui si riferisce la disposizione normativa[29].

---

[28] È peraltro opportuno rilevare che la previsione di uno specifico obbligo di tenuta da parte del responsabile del Registro delle attività di trattamento, in aggiunta a quello del titolare del trattamento, ha costituito uno degli argomenti utilizzati per affermare che la disciplina contenuta nel *GDPR* non consentirebbe la nomina di un responsabile del trattamento "interno", potendo rivestire tale posizione solamente soggetti "esterni" al titolare, mentre eventuali soggetti collocati nella struttura organizzativa o aziendale del titolare sarebbero da qualificare quali designati e autorizzati ai sensi degli artt. 29 GDPR e 2-*quaterdecies* cod. prot. dati pers. (L. GRECO, *L'organigramma privacy: i soggetti del trattamento*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* a cura di Finocchiaro, Bologna, 2019, p. 343 ss.). per quanto l'opinione in parola non sia stata condivisa da una parte della dottrina, prospettando la possibilità di differenziare la disciplina applicabile al responsabile "esterno" rispetto a quella riferibile al responsabile "interno", che sarebbe assoggettato a quella del responsabile "esterno" «nei soli limiti di quanto risulti eventualmente possibile e con gli adeguamenti che si rendono necessari in via interpretativa» (F. BRAVO, *Sulla figura del responsabile "interno" del trattamento di dati personali*, in *Dir. inf. e informatica*, 2019, p. 973, il quale – nello specifico e per quanto in questa sede rileva – afferma che «l'art. 30, par. 2, GDPR […] potrà essere applicato al responsabile interno affidando a questi la gestione della porzione di registro prevista per il titolare del trattamento ai sensi del par. 1 del medesimo articolo»), non pare che si possa convenire con tale ultima impostazione, non fosse altro che diversamente si legittimerebbe un porzionamento delle competenze relativamente ai contenuti del registro che sono considerati unitariamente dal legislatore. D'altronde, neppure sembra possibile affermare che il responsabile, qualora "interno", debba tenere il relativo registro, posto che ciò si tradurrebbe in una inutile duplicazione (v. L. GIACOMINI-C.A. TROVATO-C. ROSSI CHAUVENET, *op. cit.*, p. 457), che esporrebbe in definitiva il medesimo soggetto al rischio di essere sanzionato in quanto titolare e in quanto responsabile, ragione questa che nella realtà ha indotto le grandi realtà aziendali a non nominare responsabili "interni", preferendo qualificarli come designati al trattamento dei dati personali (su tale ultima figura, anche in relazione a quella di persona autorizzata, v. D. FARACE, *Le persone autorizzate al trattamento dei dati personali*, in *Riv. trim. dir. e proc. civ.*, 2021, p. 423 ss.).

[29] In questo senso S. MELCHIONNA, *op. cit.* p. 289, che individua il contenuto eventuale del registro del responsabile negli elementi considerati come requisiti minimi del registro del titolare non previsti dalla norma per quello del responsabile e nel contenuto ulteriore del registro del titolare (v., *retro*, nota n. 26), considerando di particolare utilità l'indicazione dell'applicazione di un codice di condotta o di un

Infine, può senz'altro convenirsi sul rilievo per cui il responsabile del trattamento sarà altresì tenuto, in ragione della contemporanea pluralità dei ruoli ricoperti, a tenere, salvo che ne resulti esentato, anche il registro delle attività di trattamento per i dati di cui è titolare, non potendosi invece condividere l'ulteriore assunto secondo cui il responsabile dovrebbe tenere tanti registri quanti sono i soggetti per i quali viene effettuato il trattamento[30]. In senso contrario a quest'ultima interpretazione depone lo stesso dato normativo, il quale parla di «un registro» e indica che questo deve contenere i riferimenti legislativi ad «ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento», con ciò suggerendo di escludere una moltiplicazione del registro anche in ossequio ad un principio di semplificazione che sembra dover ispirare un adempimento così peculiare e complesso. D'altronde, deve considerarsi che la tenuta del registro in questione è strettamente connesso all'attività svolta dal soggetto responsabile e non anche dal titolare del dato, sicché non pare avere fondamento la tesi che richiede un numero di registri pari a quello dei titolari dei dati di cui si è responsabili.

Peraltro, quanto ai rapporti tra titolare e responsabile, si è ritenuto che non sia possibile escludere un obbligo di vigilanza del primo sulla tenuta del registro da parte del secondo[31]. L'affermazione, pur da condividere, nella sua genericità potrebbe essere fuorviante, non potendosi intendere che il suddetto obbligo di vigilanza da parte del titolare sia limitato alla verifica dell'esistenza di tale registro, estendendosi piuttosto anche all'accertamento della sua regolarità formale e finanche alla corretta tenuta dei dati riguardanti l'attività di trattamento[32].

4. Le regole di tenuta e di gestione dei registri.

I registri delle attività di trattamento, secondo l'unica prescrizione circa la tenuta e la gestione dei registri in parola fornita dall'art. 30 *GDPR*, devono essere «tenuti in forma scritta, anche in formato elettronico», il che implica la possibilità di compilare il registro sia in formato cartaceo che in formato elettronico. In tale ultimo ipotesi, che, come intuibile, costituisce la stragrande maggioranza dei casi, il registro – secondo quanto indicato del Garante per la protezione dei dati personali [33] – deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento.

---

meccanismo di certificazione da parte del responsabile «in quanto tale elemento può essere utilizzato dal titolare come parametro per verificare il rispetto degli obblighi da parte del responsabile».

[30] S. MELCHIONNA, *op. cit.*, p. 285.

[31] S. MELCHIONNA, *op. loc. cit.*

[32] Si tenga al riguardo presente che nella contrattualistica che coinvolge il titolare del trattamento e il responsabile del trattamento è frequente la previsione di specifiche clausole contrattuali che attribuiscono al primo delle facoltà ispettive sulla corretta tenuta del registro da parte del responsabile del trattamento. In argomento vd. A. CHIAPPINI, *Riflessioni sul contratto tra titolare e responsabile del trattamento*, in *Contratto e impresa*, 2021, p. 317 ss.

[33] Si tratta delle già richiamate FAQ sul registro delle attività di trattamento del Garante per la protezione dei dati personali.

Oltre alla prescrizione sulla forma, che – come detto – è l'unica espressamente prevista dal dato normativo, può tuttavia ritenersi che s'impongano ulteriori regole risultanti dal sistema.

In primo luogo, le informazioni contenute nei registri devono necessariamente essere aggiornate[34], dovendo quindi essere caratterizzate dal requisito dell'attualità. In tal senso, in base alle richiamate indicazioni del Garante per la protezione dei dati personali[35], si è evidenziato che il registro dei trattamenti, in quanto documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile, deve essere mantenuto costantemente aggiornato dovendo il suo contenuto corrispondere all'effettività dei trattamenti posti in essere, da ciò derivando che qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel registro, dando conto delle modifiche sopravvenute.

Infine, deve ritenersi che ulteriori specifiche regole di tenuta e gestione dei registri sull'attività di trattamento siano costituite dalla completezza, che si collega al contenuto dei registi sia come individuati dalla normative che come necessario in base alla particolarità del caso, dalla veridicità, dovendo corrispondere quanto indicato nei registri alle reali ed effettive modalità di trattamento, e dalla intellegibilità dei dati riportati, dovendo questi avere un sufficiente grado di chiarezza di ordine interpretativo o percettivo.

5. L'obbligo di mettere a disposizione del Garante il registro.

Come accennato in precedenza, una delle funzioni principale del registro sull'attività di trattamento è quella di dare concretezza alla cooperazione dei soggetti che effettuano il trattamento con l'autorità Garante della protezione dei dati personali. Proprio in questa prospettiva, l'art. 30, par. 4, *GDPR* prevede che il titolare o il responsabile debbano mettere a disposizione delle autorità di controllo il registro delle attività di trattamento. Occorre al riguardo tenere presente che siffatto obbligo, a differenza di quanto avveniva nella previgente disciplina con riguardo alle notificazioni[36], deve essere fornito alle autorità unicamente a fronte di una specifica richiesta in tal senso. In tale contesto, peraltro, si deve rilevare che le autorità di controllo avranno in ogni caso la possibilità di richiedere, nell'ambito dei propri poteri ispettivi e di controllo, ogni ulteriore documento necessario per lo svolgimento delle proprie funzioni, non potendosi certamente ipotizzare che le richieste siano limitate al registro delle attività di trattamento.

Ciò che certamente si può rilevare è che la tenuta dei registri in parola, oltre a correlarsi al principio di responsabilizzazione, rivestono altresì un ruolo non secondario nelle attività ispettive, di monitoraggio e di vigilanza svolte dall'autorità.

---

[34] Sul punto si è ritenuto che «l'aggiornamento […] debba avvenire in tempo reale […], tanto da divenire una sorta di obbligo dinamico» (così S. MELCHIONNA, *op. cit.*, p. 289).

[35] V. le FAQ sul registro delle attività di trattamento cui si è in precedenza fatto riferimento.

[36] Il rilievo si trova in S. MELCHIONNA, *op. cit.*, p. 291.

6. Le esenzioni.

A fronte del generico obbligo di tenuta dei registri del trattamento, l'art. 30, par. 5, *GDPR* prevede una serie di esenzioni che escludono l'obbligatorietà di tale adempimento per terminati soggetti, vale a dire le imprese o le organizzazioni con meno di 250 dipendenti, salvo il caso che il trattamento effettuato possa presentare un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di categorie particolari di dati personali (art. 9, par. 1, *GDPR*) o di dati personali relativi a condanne penali e a reati (art. 10 GDPR). In altri termini, a fronte dell'esenzione per i soggetti con caratteristiche dimensionali inferiori a 250 dipendenti[37], la norma individua tre ipotesi che consentono di escludere l'operatività dell'esenzione facendo quindi riemergere l'obbligatorietà della tenuta del registro delle attività di trattamento per imprese o organizzazioni[38], vale a dire: a) il rischio per i diritti e le libertà dell'interessato; b) la non occasionalità del trattamento [39]; c) l'utilizzo di particolari categorie di dati personali.

Con specifico riferimento al rischio per i diritti e le libertà dell'interessato come anche alle particolari categorie di dati personali, a fronte dell'indeterminatezza dei concetti, un utile parametro di riferimento per le valutazioni del caso è costituito dal Considerando n. 75, il quale si riferisce a «i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;

[37] Si tenga presente che il Considerando n. 13 afferma che «Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni».

[38] Il riferimento alle imprese e alle organizzazioni induce ad escludere dall'ambito di applicazione dell'esenzione i soggetti pubblici (in questo senso v. S. MELCHIONNA, *op. cit.*, p. 285, che giunge a tale conclusione anche in ragione dell'ambito oggettivo dell'esenzione che non consentirebbe di includervi i soggetti pubblici).

[39] Segnala S. MELCHIONNA, *op. cit.*, p. 286, che «l'Autorità di controllo belga (*Commission de la protection de la vie privée* – CPVP), al fine di fornire utili elementi interpretativi, ha richiamato la definizione inglese del termine occasionale, arrivando a suggerire di considerare occasionali quei trattamenti che si verificano a intervalli irregolare o sporadici, ovvero di tanto in tanto o per caso [Raccomandazione n. 6 del 14 giugno 2017 della CPVP, punto 18]».

se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati». Si tratta, com'è facile intuire, di una elencazione non tassativa, ben potendosi far riferimento ad ulteriori ipotesi che consentono di neutralizzare l'esonero dall'obbligo di tenuta del registro delle attività di trattamento, dovendosi più in generale ritenere che la deroga non possa operare tutte le volte in cui sussiste un potenziale pregiudizio ai diritti e alle libertà personali dei soggetti cui i dati personali si riferiscono.

Certamente di più difficile determinabilità è il riferimento alla non occasionalità del trattamento, con riguardo al quale nella valutazione di non saltuarietà e, quindi, di ricorrenza del trattamento, si dovrà pur sempre tenere in considerazione che si tratterà di un'analisi prognostica da compiere sulla ragionevole previsione della ricorrenza del trattamento, senza che possano assumere rilevanza le contingenze del caso concreto che non siano preventivamente correlabili al trattamento realmente effettuato.

La maggiore difficoltà interpretativa che si è riscontrata nell'individuazione dell'ambito di applicazione dell'esenzione in parola ha riguardato la portata delle tre richiamate condizioni di esclusione dell'esenzione, con riferimento alle quali si sono prospettate due opzioni ermeneutiche, da un lato ritenere che le condizioni in parola siano tra loro alternative e, pertanto, anche solo una di esse renda inoperante l'esenzione dall'obbligo di tenuta dei registri, dall'altro lato ritenere che le tre condizioni operino in maniera composita, ipotizzando che oltre al rischio per diritti e libertà dell'interessato l'esclusione della esenzione richiede che sussistano o la non occasionalità del trattamento o l'utilizzo di particolari categorie di dati[40].

Sul punto, la formulazione letterale della norma e le preposizioni che la compongono inducono a ritenere che il requisito primario di esenzione, costituito dalla struttura dimensionale dell'impresa o dell'organizzazione, che non deve avere più di 250 dipendenti, sia irrilevante e quindi il soggetto sarà comunque obbligato alla tenuta del registro dell'attività di trattamento, nel caso in cui sussista anche una delle tre condizioni di esclusione dell'esenzione (rischiosità del trattamento, trattamento non occasionale o trattamento di dati particolari), come conferma l'uso della congiunzione "o" tra il secondo ed il terzo caso previsi dalla norma[41]. Tale interpretazione, pur rendendo di fatto applicabile l'esenzione ad un ristretto e limitato numero di ipotesi, con la conseguenza che la tenuta dei registri dell'attività di trattamento risulta obbligatoria nella quasi totalità dei casi, è l'unica che risulta conforme al dato letterale e sistematico, non potendosi ammettere differenti letture, quale, in

[40] Rileva S. MELCHIONNA, *op. cit.*, p. 285, che inizialmente la lettura composita è stata prospettata dall'Autorità di controllo tedesca (*Unabhängige Landeszentrum für Datenschutz (ULD), Kurzpapier Nr. 1 – Verzeichnis von Verarbertunstätigkeiten* – Art. 30 DS-GVO, del 29 settembre 2017).

[41] In tal senso si è espresso anche il *Position Paper on the dergations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR* del Gruppo di lavoro Articolo 29 del 19 aprile 2018, il quale ha ritenuto che «the wording of Article 30(5) is clear in providing that the three types of processing to which the derogation does not apply are alternative ("or") and the occurrence of any one of them alone triggers the obligation to maintain the record of processing activities». In questo senso si è peraltro orientato il Garante per la protezione dei dati personali nel provvedimento n. 278 del 17 dicembre 2020 (doc. web n. 9529527), dove si è affermato che «la deroga alla tenuta del registro prevista dal Regolamento non opera in presenza anche di uno solo degli elementi indicati dall'art. 30, par. 5 (trattamento che presenta un rischio per i diritti e le libertà dell'interessato, trattamento non occasionale, trattamento che includa categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati)».

particolare, quella che al fine di escludere l'operatività dell'esenzione richiede contemporaneamente che il trattamento presenti un rischio per i diritti e le libertà dell'interessato e che il trattamento sia o non occasionale o riguardante dati particolari/giudiziali[42]. D'altronde, non può essere nascosto il *favor* verso i registri delle attività di trattamento manifestato dal Garante per la protezione dei dati personali, il quale ha auspicato che i titolari del trattamento e i responsabili del trattamento si adoperino per la tenuta dei registi indipendentemente dai propri requisiti dimensionali[43].

7. I registri come strumenti di valutazione e documentazione della conformità del trattamento al GDPR.

Quanto sinora detto consente di confermare che la tenuta dei registri della attività di trattamento risulta complementare all'attuazione del principio di responsabilizzazione, costituendo altresì un indispensabile strumento di cooperazione con il Garante per la protezione dei dati personali, dovendosi peraltro attribuire ai registri in questione una ulteriore e non marginale funzione laddove gli stessi consentono di determinare la conformità del trattamento alla normativa in tema di protezione dei dati personali.

Una chiara indicazione in tal senso sembra desumibile dai primi provvedimenti di ingiunzione del Garante per la protezione dei dati personali relativi all'art. 30 *GDPR,* dove si è affermato che i «registri […] sono indispensabili per consentire di valutare e documentare la conformità dei trattamenti alla disciplina in materia di protezione dei dati personali e dunque sono preliminari rispetto all'avvio degli stessi»[44].

Per quanto tale rilevanza attribuita ai registri sembra andare oltre quanto indicato dall'art. 6 *GDPR* laddove si individuano le condizioni di liceità del trattamento con una formulazione che difficilmente consente di riferirsi all'adempimento di cui all'art. 30 *GDPR,* una differente conclusione si giustifica ricordando che l'obbligo di tenuta del registro dei trattamenti costituisce un prerequisito dell'attività di trattamento laddove consente di soddisfare la responsabilizzazione della stessa, risultando finanche funzionale all'obbligo di garantire l'adeguatezza delle misure di sicurezza e protezione dei dati personali[45], con ciò dando concretezza al nesso inscindibile che il legislatore europeo ha voluto costituire tra il processo di gestione dei dati personali e la liceità del loro trattamento.

---

[42] Così, ad esempio, G. ARCELLA, *GDPR: il registro delle attività di trattamento e le misure di* accountability, in *Notariato*, 2018, p. 393.

[43] In tal senso si esprime la già citata Guida per l'applicazione del Regolamento europeo in materia di protezione dei dati personali emanata dal Garante per la protezione dei dati personali, dove «si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro» (p. 26).

[44] Il riferimento è al provvedimento n. 268 del 21 luglio 2022 (doc. web n. 9811271), ma in senso non dissimile, ancorché senza riferirsi alla idoneità a «documentare la conformità al trattamento», i provvedimenti nn. 292 e 293 del 22 luglio 2021 (doc. web nn. 9698558 e 9698597), n. 134 del 7 aprile 2022 (doc. web n. 9768363).

[45] Su questo punto si rivela particolarmente interessante la recente pronuncia della Corte di Giustizia UE 14 dicembre 2023, C-340/21, *VB* c. *Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986, in *Foro it.*, 2024, IV, c., 58 ss. Sul tema vd. A. MONTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Leggi civ. comm.*, 2017, p. 144 ss.; ID., *La gestione del rischio*, in *La protezione dei dati personali in Italia*, cit., p. 473 ss.

A tale riguardo sembra imprescindibile riscoprire una prospettiva non sempre adeguatamente considerata dagli interpreti, vale a dire quella che muovendo dal nesso intercorrente tra riservatezza e diritto alla tutela dei dati personali chiarisce che quest'ultimo costituisce «una distinta figura di diritto della personalità, in quanto l'interesse a non subire un abusivo trattamento dei dati personali è esso stesso un distinto interesse della persona»[46].

In questo contesto, l'obbligo di tenuta del registro dell'attività di trattamento esplicita quel necessario bilanciamento tra diritto all'informazione e diritto alla riservatezza che, oggi come ieri, sottende alla normativa sulla tutela dei dati personali e che deve essere assunto quale «punto fermo di orientamento per l'interprete»[47], rivelando in definitiva la sua centralità nel vigente quadro normativo e regolamentare della protezione dei dati personali.

[46] C.M. Bianca, *I. Note introduttive*, in *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)*, cit., p. XXII, e in termini non dissimili anche Id., *Il diritto alla riservatezza*, già in *Valore della persona e giustizia contrattuale. Scritti in onore di Adriano de Cupis*, Milano, 2005, p. 37 ss., e più di recente in Id., *Realtà sociale ed effettività della norma*, Torino, 2023, p. 89 ss. e spec. p. 96.
[47] C.M. Bianca, *I. Note introduttive*, cit., p. XXXI.

Murgo C, 'L'identità personale dei minori, tra responsabilità genitoriale e capacità di autodeterminarsi' (2024) 2 EJPLT, 115-128.
DOI: https://doi.org/10.57230/EJPLT242CM

EJPLT
ISSN 2704-8012



L'identità personale dei minori, tra responsabilità genitoriale e capacità di autodeterminarsi

The personal identity of minors, between parental responsibility and the capacity for self-determination

CATERINA MURGO
Professoressa Associata di Diritto Privato
Università degli Studi di Pisa

Abstract

Il contributo è rivolto all'esame delle questioni connesse con il trattamento dei dati personali riferibili a soggetti minori d'età. Nell'ordinamento interno e sovranazionale i minori ricevono forme di tutela specifica in considerazione del loro status e degli ambienti ove si trovano a operare. Il legislatore delinea le situazioni in cui i minori sono legittimati a compiere atti di natura personale alla luce delle singole capacità di scelta. Diversamente, i poteri decisionali ricadono sui genitori, per i quali vige l'obbligo di tenere conto dell'età, delle capacità e delle inclinazioni del minore.

The paper aims to make a focus on the people under eighteen age and the dealing of their personal data. These people are receiving a special protection by the law in all the sets where they live. The law says when the minors have been allowed to make some personal acts due to their ability and when their parents can decide instead of the children, even including the consideration of their age and the own skills. The giving consent to the treatment of the personal data by the under eighteen people is a difficult matter, while both the national law and the European legal acts try to set some effective rules for all the families.

* Il presente contributo è destinato allo special issue in memoria del Prof. Cesare Massimo Bianca e del Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy» da lui curato con il Prof. Francesco Donato Busnelli nel 2007 (Cedam).

© The author(s) 2024, 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: minori; responsabilità genitoriale; condivisione dei dati

Summary: Introduzione. – 1. Soggetti minori d'età e trattamento dei dati personali. – 2. I minori nell'ordinamento, tra capacità legale e manifestazione della volontà. – 3. Responsabilità genitoriale, diffusione dei dati personali della prole e tutele normative.

Introduzione.

L'accesso dei minori alle opportunità offerte dalle nuove tecnologie rappresenta uno spazio, sociale e giuridico, idoneo a includere molteplici profili, tutti egualmente rilevanti e ulteriormente declinabili, in quanto modellati sul bilanciamento tra la protezione della persona del minore e l'*enhancement* della posizione di soggetti che sono fisiologicamente in fase di formazione e di crescita[1].

In particolare, l'attivazione e la gestione da parte dei minori dei contenuti propri dei servizi offerti dalle piattaforme digitali sollecitano la riflessione non soltanto sui risvolti psicologici, ambientali e di tipo educativo, ma anche sui presupposti giuridici che conferiscono legittimità alla condotta dei minori.

La valorizzazione del procedimento di formazione ed esternazione della volontà del minore caratterizza tutti i formanti dell'ordinamento, da quello normativo all'articolazione nell'ambito delle decisioni delle corti, fino a connotare la riflessione giuridica sul tema e a coinvolgere i principali contesti di riferimento della categoria, dalla famiglia alla scuola, per giungere alla rete amicale tra pari.

Anche l'angolo di visuale su cui può appuntarsi il *focus* appare variamente articolato: *a*) si registra un costante incremento delle potenzialità, ma anche dei rischi connessi all'uso dei *tools* digitali da parte dei soggetti minori d'età: è quanto ribadito dall'Autorità Garante nel testo dei provvedimenti dedicati al tema della tutela di quanti rientrano nella fascia d'età under diciotto, laddove i gestori dei servizi hanno da tempo individuato nei minori uno dei versanti, fra i destinatari di diritti e di obblighi, ad alto potenziale di attenzione[2].

b) L'inquadramento che guarda ai minori come beneficiari di specifiche forme di protezione induce a ulteriori considerazioni sull'estensione potenziale dell'ambito della tutela, che deve essere rivolta non soltanto avverso le condotte dei terzi estranei al nucleo familiare, ma è chiamata ad attivarsi anche in presenza di attività pregiudizievoli di provenienza endofamiliare.

[1] Sul tema, v. *Commento generale* n. 25 adottato dal Comitato delle Nazioni unite, 18 gennaio-5 febbraio 2021, sui diritti dei minori nello spazio digitale: di particolare interesse il punto IV, che delinea un modello di azione adattabile all'evoluzione fisica e mentale dei minori, e il punto VI, sull'esercizio dei diritti connessi all'accesso ai servizi digitali. Il commento n. 25 delle Nazioni Unite si legge sul sito: *https://www.garanteinfanzia.org/sites/default/files/2022-02/commento-generale-25-web.pdf*.
Per le ricadute negative sulla libera manifestazione del pensiero, M. CIANCIMINO, *La libertà di espressione nel mondo digitale: alcune coordinate civilistiche in tema di contenuti controversi sui social network*, in *Dir. fam. per.*, 2022, 360-389.

[2] Indicazioni utili sul tema possono leggersi al seguente indirizzo: *www.garanteprivacy.it/temi/minori*.

Sul tema, anche la recente riforma del processo civile, istitutiva di un organo giudiziario unico per i procedimenti inerenti alla persona, ai minorenni e alle famiglie, è stata orientata all'emersione e valorizzazione dell'interesse del minore in tutti i procedimenti idonei a coinvolgerlo, come confermato dalle tematiche inerenti alla rappresentanza processuale ovvero, in qualche caso, anche sostanziale della persona del minore[3].

c) con riguardo all'esercizio dei diritti personalissimi, l'eventuale conflittualità tra il minore e quanti esercitano le funzioni genitoriali richiede soluzioni che coniughino la disciplina speciale e le norme proprie del diritto della famiglia che regolano le molteplici declinazioni dei rapporti familiari, dalla relazione tra gli adulti di riferimento al legame con i discendenti.

L'oggetto del presente lavoro prende spunto dall'esame di una pratica, il c.d. *sharenting*, oggetto di particolare diffusione nel contesto sociale attuale, fondata sulla condivisione di riproduzioni digitali che interessano soggetti minori d'età, foto e video in particolare, da parte di quanti esercitano la responsabilità genitoriale.

Motivazioni differenti sono all'origine del fenomeno: dalla prima ecografia fino al conseguimento dei più alti titoli di studio e all'ingresso nella sfera professionale e lavorativa, i genitori fanno fatica a rinvenire limiti al proprio bisogno di condividere i dati inerenti ai figli, anche ben oltre il conseguimento del diciottesimo anno.

E tuttavia, è proprio la minore età la fascia temporale densa di maggiori criticità, laddove l'individuo è in fase di formazione e necessita di acquisire le nozioni e di gestire le competenze utili a muoversi sulla scena reale e in quella virtuale.

È in questa fase che l'istituto della responsabilità genitoriale deve necessariamente modellarsi sulla persona dei minori e sulla sua costruzione, riempiendo di nuovi significati e contenuti i doveri educativi, di formazione e di assistenza morale e materiale.

La condotta incentrata sullo sharenting produce l'effetto di esternalizzare i dati dei minori rispetto al contesto originario della circolazione, diffondendoli ovvero contribuendo alla loro diffusione presso soggetti terzi e sottraendo i dati all'esercizio di poteri di controllo effettivi da parte dell'interessato. Si tratta, inoltre, di una modalità operativa che ingenera dubbi sulla reale partecipazione dei minori rispetto al procedimento di circolazione dei propri dati e sollecita l'intervento dell'ordinamento nell'ipotesi, possibile, di trattamento dei dati identificativi e contestuale violazione dei doveri inerenti all'esercizio delle funzioni genitoriali.

1. Soggetti minori d'età e trattamento dei dati personali.

Le operazioni di trattamento e di circolazione dei dati personali sono

[3] A. THIENE, *Dalla parte delle famiglie per un diritto minorile gentile*, in *Dir. fam. per.*, 2023, 1315-1340. Sul curatore speciale del minore, P. MACCARONE, *nota a* Trib. Bergamo, 09.05.2022, n. 1107, sez. I, in *ilfamiliarista.it*, 22 settembre 2022, par. Osservazioni, consultabile al sito *De Jure.* Per la riforma del processo civile, C. CECCHELLA, *Il tribunale per le persone, per i minorenni e per le famiglie della legge delega di riforma del processo civile*, in *Questione Giustizia* 2021, fasc. 3, 239-248.

strettamente connesse con la protezione dei "diritti e (del)le libertà fondamentali delle persone fisiche", secondo quanto recita il par. 2, art. 1 del Reg. UE 2016/679, sulla protezione dei dati personali, norma che non distingue tra i titolari dei diritti in considerazione dell'età[4].

In un *habitat* connotato dal ricorso massiccio ai dispositivi digitali, l'ordinamento rincorre la tecnologia, predisponendo forme di regolamentazione a garanzia della tutela della persona e, al tempo stesso, in funzione dell'accesso ai benefici offerti dalle risorse *on line* in favore di una platea il più possibile inclusiva, anche in ragione del grado di diffusione raggiunto dall'offerta negoziale di beni e servizi.

Se la riflessione giuridica si interroga sulla valenza del consenso al trattamento dei dati personali da parte dell'interessato, presupposto che sia la l. 675/1996, sia il d. lgs. 196/2003 avevano individuato come centrale nel testo della disciplina[5] e che in seguito è stato rimodellato dal regolamento europeo del 2016[6], il profilo consensualistico, nel più vasto ambito delle operazioni di trattamento dei dati, presenta ulteriori sfumature di criticità nel caso di dati personali riconducibili ai minori d'età, in considerazione della duplice veste di soggetti attivi dell'ordinamento, in quanto fascia consumeristica di riferimento per le compagnie di distribuzione di beni e dispositivi, e di categoria protetta, alla luce delle misure di tutela predisposte dal sistema[7].

La capacità di esplorare le funzionalità digitali offerte dal mercato consente al minore di accedere ai servizi, ma anche di sperimentare tutte le articolazioni delle situazioni giuridiche inerenti alla persona: l'esercizio del potere decisionale sulle attività di condivisione dei dati presso i terzi, il diritto alla

---

[4] Sul diritto alla riservatezza in quanto espressione di un diritto di libertà della persona, R. Russo, *Diritto alla riservatezza e all'oblio: la giurisprudenza della corte di Cassazione, coerenza e limiti*, in *Questione Giustizia*, 20 giugno 2024, par. 2. Favorevole all'utilità, in ambito europeo, dell'approccio ai diritti fondamentali in un sistema regolato dal mercato, M. Dawson, *The governance of EU fundamental rights*, Cambridge University Press, 2017, 185 ss.

[5] F.D. Busnellli- C.M. Bianca (a cura di), *La protezione dei dati personali. Commento al D. Lgs. 30 giugno 2003, n. 196, ("Codice dei dati personali")*, Padova, 2007.

[6] Sul tema. A.R. Popoli, *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, in *Dir. Inf.,* 2019, 1289-1321, specie 1297 ss., e 1305 ss. sul consenso del minore.

[7] V. in materia le Linee Guida dell'Agicom, adottate con provvedimento 9/23, entrate in vigore a partire dal 21 novembre 2023, che hanno imposto agli operatori della rete l'attivazione di misure di parental control a fronte dell'accesso ai servizi da parte di soggetti minori d'età, in attuazione di una consultazione pubblicata avviata con delibera n. 16/22, in esecuzione di quanto previsto dall'art. 7 *bis* d.l. 28/2020, convertito in l. 70/2020, sui sistemi di protezione dei minori dai rischi del cyberspazio. Le linee Guida possono leggersi sul sito *agicom.it/documents*.
Sull'obbligo per i produttori e per i fornitori di servizi di comunicazione elettronica di includere meccanismi di controllo parentale, come previsto dal d.l. 123/2023, art. 13 co. 2, e in conformità del regolamento 2022/2065/UE del Parlamento europeo e del Consiglio, relativo a un mercato unico dei servizi digitali, R. Senigaglia, *L'identità personale del minore di età nel cyberspazio tra autodeterminazione e parental control system*, in *Nuove leggi civ. comm.*, 2023, fasc. 6, 1568-1602, specie 1589 ss.: l'A. prospetta un quadro connotato da una fase costruttivo/evolutiva della personalità del minore e una con finalità conservative, suggerendo di adeguare in ragione di ciò le misure d'intervento. Sui fornitori di servizi di media diffusi mediante canali o piattaforme grava l'ulteriore obbligo di conformarsi al Codice di autoregolamentazione media e minori, da adottarsi entro il 31 dicembre 2024 (art. 37, co. 6, d. lgs. 208/'21, e successive modifiche, in attuazione della dir. 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, sulle modifiche alla precedente direttiva 2010/13/UE, inerente al coordinamento della disciplina degli Stati membri sul testo unico per la fornitura di servizi di media audiovisivi). La proposta di legge A.C. 1800, all'art. 1, propone l'inserimento di un co. 8 bis all'interno dell'art. 37, d.lgs. 208, introducendo l'obbligo per gli esercenti la responsabilità genitoriale di effettuare una comunicazione all'AGCOM in caso di diffusione di materiale audiovisivo su piattaforme che abbia come soggetto principale o quale compartecipe un minore di anni quattordici, indicando se l'operazione persegue finalità lucrative.

libera manifestazione del pensiero e quello a prendere parte alle formazioni sociali ove trova spazio la personalità del singolo, sia pure in forma soltanto virtuale, rappresentano soltanto alcune tra le manifestazioni più significative a cui il minore può accedere[8].

Come rilevato dalla dottrina nell'ambito del dibattito sulla qualificazione del consenso al trattamento dei dati da parte della persona under eighteen, si tratta di una vicenda ove intervengono profili patrimoniali e, al contempo, personalissimi[9].

L'introduzione del minore ai servizi offerti dai gestori determina l'effetto di immettere *on line* un imponente complesso di dati, anche sensibili, inerenti alla persona minore d'età, in conseguenza della sua stessa condotta, più o meno consapevole, ovvero in considerazione della diffusione dei dati che riguardano il minore da parte di attori ulteriori, quali i familiari, le comunità scolastiche, i complessi sociali che operano in ambito sportivo o di svago, enti, piattaforme, la rete amicale[10].

Sul tema del trattamento dei dati personali ove siano coinvolti soggetti minori, l'ordinamento ha registrato un'evoluzione nell'approccio di base: dall'assenza di indicazioni peculiari sul trattamento dei dati inerenti ai minori nel testo della l. 675/1996, si è pervenuti, con l'approvazione del d. lgs. 196/2003, c.d. Codice della *privacy*, alla formulazione dell'art. 50 del Codice, che contempla l'estensione del divieto di diffusione di notizie e immagini sul minore anche al di fuori del procedimento penale, come previsto dal D.P.R. 448/1988, oltre che alla previsione di cui all'art. 52 co. 5 d. lgs. 196, che impone l'omissione di dati idonei a identificare il minore nei provvedimenti giurisdizionali[11].

Il regolamento europeo del 2016 n. 679 ha inquadrato l'accesso dei minori ai servizi digitali tra le articolazioni maggiormente delicate della materia, riservandovi spazio, oltre che in alcuni dei considerando, nello specifico ai nn. 38, 58, 71, 75, principalmente all'art. 8, dedicato alle condizioni applicabili al consenso al trattamento, ma anche in altre disposizioni, quali l'art. 6 co. 1, lett. f, sulla liceità del trattamento; l'art. 12, co. 1, sulle modalità degli obblighi di informativa; l'art. 40, co. 2, lett. g, sui codici di condotta interni ai singoli Stati; l'art. 57, co. 1, lett. b, sui compiti propri delle autorità di controllo.

Trovano inoltre applicazione anche agli under eighteen le ulteriori previsioni sulla liceità del trattamento di cui all'art. 6 del regolamento, nei limiti dell'applicabilità a un soggetto minore d'età, e l'art. 7, norma che disciplina le condizioni necessarie per la prestazione del consenso.

L'art. 8 del regolamento, in particolare, collocando, al par. 1, a sedici anni la soglia utile per la prestazione del consenso al trattamento dei dati da parte dei minori in relazione ai servizi della società dell'informazione offerti in via diretta, ha sollevato il velo su forme di tutela che si rivelerebbero prive di efficacia in

[8] Il commento generale ONU n. 25, cit., tra i principi generali, oltre all'esigenza fondamentale di protezione dei minori, disegna anche il dovere gravante sugli Stati di impedire condotte discriminatorie nella fase preliminare dell'accesso ai servizi digitali, riconducendo alle omissioni degli organismi pubblici la fonte di nuove possibili diseguaglianze.

[9] C. Irti, *Persona minore di età e libertà di autodeterminazione*, in *Giust. civ.*, 2019, fasc. 1, 617 ss., par. 1.

[10] E. Adamo, *L'identità del minorenne nella rete, tra istanze di protezione e prospettive rimediali*, in *Dir. fam. per.*, 2023, 1677-1709; E. Battelli, *Il trattamento dei dati nel prisma della tutela della persona minore d'età, in Dir. inf.,* 2022, 267-301, specie 268, ove si parla di processo di "datafication".

[11] F. Naddeo, *Il consenso al trattamento dei dati personali del minore*, in *Dir. inf.*, 2018, 27-64, specie 34 ss.

concreto, ingenerando dubbi sull'effettiva libertà dell'intera operazione [12]; nella prassi, infatti, il consenso è offerto in cambio dell'accesso a prestazioni considerate generalmente essenziali dagli utenti, oltre che essere caratterizzato da possibili fraintendimenti sulla determinazione del suo oggetto[13].

La medesima disposizione fa salva la liceità del consenso prestato dagli esercenti la responsabilità genitoriale per i soggetti infrasedicenni ovvero di età inferiore, se l'ulteriore abbassamento dell'età sia previsto dalle singole legislazioni nazionali[14].

Per l'Italia, secondo quanto disposto dall'art. 2 *quinquies* co. 1 d. lgs. 196/2003, l'età richiesta per le finalità di cui all'art. 8 par. 1 del regolamento è quella corrispondente a quattordici anni, delineando al co. 2 il legislatore il contenuto degli obblighi informativi gravanti sui gestori al fine di rendere effettivo il consenso prestato.

La soglia d'età dei quattordici anni è la medesima contemplata dalla normativa sulla tutela dal cyberbullismo, l. 71/2017: in tale ambito, la dottrina ha denunciato un vero e proprio depotenziamento della tutela determinato dall'opzione normativa che consente soltanto ai minori ultraquattordicenni di attivarsi in via diretta, a cui si aggiungono gli esercenti la responsabilità genitoriale (art. 2 co. 1, l. 71)[15]. In relazione alla normativa, le perplessità sono state sollevate in particolar modo in considerazione della diffusione del fenomeno, connotato da condotte persecutorie on line anche tra minori di età inferiore a quanto previsto dalla legge e alla luce delle comuni esigenze educative sull'uso dei social media e sul godimento dei servizi offerti dai gestori[16].

La previsione di cui all'art. 8 del regolamento distingue inoltre, al par. 3, l'età utile a rilasciare il consenso al trattamento e quella singolarmente prevista dalle legislazioni nazionali a fini negoziali, che non è pregiudicata per quanto attiene alla validità, formazione, efficacia dei contratti inerenti ai minori: come rilevato da più parti, sul punto, nonostante l'apparente chiarezza della norma, non sarebbe di fatto consentito operare quella netta biforcazione che il sistema

---

[12] Sull'opportunità di uniformazione della materia, G. CAPILLI, *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, in *MediaLaws*, 2024, 1 ss., specie 5 ss.

[13] E. ADAMO, *L'identità del minorenne nella rete, tra istanze di protezione e prospettive* rimediali, *op. cit.*, 1683 ss.

[14] Il Children's On Line Privacy Protection Act, approvato negli USA nel 1998, riferisce il termine child alle persone di età inferiore a 13 anni, riconducendo gli altri soggetti, quelli compresi nella fascia quattordici-(quasi) diciotto, alla categoria dei minors. La previsione di tutele specifiche per i soggetti under thirteen è stata confermata dal Bill to protect the safety of children on the internet, del 2023, che, alla sec. 2, Definitions, prevede che "The term "child" means an individual who is under the age of 13": il documento è consultabile al sito https://www.congress.gov/118/bills/s1409/BILLS-118s1409rs.pdf.

[15] [15] G. CASSANO, C. MARVASI, commento a Trib. Sulmona, 9 aprile 2018, n. 103, in *Danno. resp.*, 2018, fasc. 6, 765-771.

[16] G. CASSANO, C. MARVASI, op. cit., 766. La configurazione di un'apposita categoria composta dai minori ultraquattordicenni è stata rimodellata sia dalla riforma sullo stato giuridico dei figli, con la l. 219/'12 e il d. lgs. 154/'13, sia dalla normativa di attuazione della legge delega sulla riforma del processo civile, l. 206/'21. Basti pensare alle modifiche introdotte in tema di *status filiationis*, con riguardo al potere di attivazione del minore, agli artt. 244, 248, 249, 250, 264 c.c., e all'art. 273 co. 2 c.c., in materia di accertamento giudiziale del legame di filiazione. Si legga anche, sulla nomina e l'eventuale revoca del curatore speciale da parte del minore, la previsione di cui all'art. 473 *bis.*5 c.p.c., in attuazione di quanto disposto dall'art. 473 *bis.*8, co. 1, lett. d, norme introdotte nel codice procedurale dal d. lgs. 149/'22.

richiede[17]. La manifestazione della volontà al trattamento coinciderebbe con l'adesione all'offerta negoziale del bene o servizio fruibile, ingenerando una vivace riflessione giuridica sulla commistione tra l'efficacia del consenso e la libertà del soggetto di disporre di risorse personalissime, quali sono i dati personali[18].

A completare il quadro, come rilevato dalla dottrina, intervengono norme la cui fonte è interna ovvero di provenienza sovranazionale, quali l'art. 10 c.c., che detta regole generali sul diritto all'immagine e sull'azione in funzione inibitoria a sua tutela[19]; le previsioni della l. 633/1941, artt. 96 e 97, che definiscono i presupposti funzionali alla circolazione dell'immagine della persona; l'art. 32 della Convenzione di New York del 1989, che protegge i minori contro lo sfruttamento economico e assicura in favore degli stessi la garanzia di adeguate condizioni lavorative, ove l'ordinamento ammetta il lavoro minorile[20].

2. I minori nell'ordinamento, tra capacità legale e manifestazione della volontà.

La condizione dei minori d'età è da tempo oggetto di un importante ripensamento da parte della dottrina e della giurisprudenza: entrambi i formanti hanno affiancato i minori nel difficile passaggio da meri destinatari di processi decisionali altrui alla partecipazione attiva in ambito familiare e nel contesto sociale nel quale sono collocati[21].

In posizione intermedia tra gli istituti giuridici che qualificano la persona fisica, tra capacità giuridica e capacità legale d'agire, i minori sono stati tra i protagonisti delle riforme più recenti del diritto della famiglia, pur in assenza di un intervento organico in grado di qualificare in via sistematica la posizione di tali soggetti dell'ordinamento, definendone idoneità e competenze anche alla luce delle soluzioni suggerite dalla comparazione con altri ordinamenti[22].

Tale categoria continua, pertanto, a muoversi tra le specifiche abilità dei singoli, quali quelle che consentono ai minori di accedere e gestire rapidamente le risorse e le attività on line[23], oltre che di compiere atti della vita quotidiana

---

[17] G. CAPILLI, *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, *op. cit.*, 8; ID., *La capacità negoziale dei minori. Analisi comparata e prospettive di riforma*, Torino, Giappichelli, 2012.

[18] E. BATTELLI, *Il trattamento dei dati nel prisma della tutela della persona minore* d'età, op. *cit.*, 275 ss., che prospetta la questione dell'interdipendenza tra il consenso al trattamento e quello negoziale, in particolare in caso d'invalidità del contratto, in adempimento a quanto previsto dalla normativa interna.

[19] Trib. Mantova, 19.09.2017, in *De Jure*.

[20] E. MOROTTI, *Il dissenso del minore alla pubblicazione della sua immagine in rete*, in *rivistafamilia.it*, del 19 gennaio 2023, che rinvia al contenuto dell'art. 16 della Convenzione di New York del 1989, ove si tutela il fanciullo da indebite interferenze nella vita privata e da fatti che possano ledere il suo onore o la sua reputazione. Sul tema, Trib. Chieti, sent. 21.07.2020, n. 403, in *De Jure*, che ha rimesso alla volontà del minore diciassettenne tutte le decisioni inerenti alla pubblicazione della sua immagine sui social.

[21] E. MOSCATI, *Il minore nel diritto privato, da soggetto da proteggere a persona da valorizzare (contributo allo studio dell' "interesse del minore")*, in *Dir. fam. per.*, 2014, 1141-1159. Per una riflessione sul "conflitto tra protezione e circolazione", L. BOZZI, *I dati del minore tra protezione e circolazione. Per una lettura non retorica del fenomeno*, in *Eur. dir. priv.*, 2020, 251-275.

[22] A. BATUECAS CALETRÌO, *Nuove tecnologie e protezione del minore nel diritto privato spagnolo*, in *Eur. dir. priv.*, 2020, fasc. 4, 1213-1257.

[23] Lo "sviluppo delle competenze digitali degli studenti, con particolare riguardo al pensiero computazionale, all'utilizzo critico e consapevole dei social network e dei media" è individuato tra gli

off line, e la capacità, da parte del sistema giuridico, di costruire una rete di garanzie che, a livello interno e sovranazionale, sia in grado di assicurare un livello esteso di protezione.

All'evoluzione della posizione del minore corrisponde una riflessione allo stesso modo produttiva sul ruolo riconosciuto a quanti esercitano le funzioni genitoriali.

L'ordinamento ha rimodellato la responsabilità genitoriale sui corrispondenti diritti vantabili dai figli, secondo il c.d. catalogo inserito nel testo dell'art. 315 *bis* c.c.: tra gli obblighi degli ascendenti, la riforma sullo *status filiationis* del 2012/2013 ha introdotto quello all'assistenza morale, che da un lato richiama la terminologia giuridica propria dei doveri matrimoniali, di cui all'art. 143 c.c., e, d'altra parte, evoca modalità d'intervento maggiormente funzionali alla personalità dei figli, quella stessa personalità che è destinata ad emergere dall'esercizio del diritto dei discendenti a essere ascoltati[24].

L'andamento della relazione genitori/figli si pone con modalità critiche in relazione all'esercizio dei diritti personalissimi, laddove si guarda con circospezione alle forme d'intervento di tipo sostitutivo a latere genitoriale, in particolare ove ci si debba relazionare con soggetti dotati di capacità di discernimento[25].

I genitori sono chiamati ad agire nell'interesse del minore, della cui posizione sono formalmente legittimati a farsi portatori: il coinvolgimento genitoriale rinviene tuttavia un limite nelle garanzie poste dal sistema giuridico in funzione di valorizzazione della volontà del minore, laddove sia possibile, in considerazione dell'età, del grado di maturità, della capacità da quello dimostrata di leggere gli eventi familiari e il contesto ambientale e personale, assumendo una posizione che definisca e identifichi il proprio pensiero.

E' quanto accade, in particolare, nella fase deliberativa inerente alle scelte che intervengono sulla salute: l'art. 3, co. 2, l. 219/2017, accogliendo un'opzione che si discosta da quanto in precedenza rilevato in tema di consenso al trattamento dei dati personali, prevede che la scelta sia manifestata da quanti esercitano le funzioni genitoriali, i quali sono chiamati a tenere conto della volontà del minore in relazione alla sua età e al grado di maturità e perimetrando il legislatore l'esercizio del potere decisionale in funzione della tutela della salute psico-fisica della persona minore e della sua dignità.

Se, per un verso, può riconoscersi che in questa occasione l'ordinamento è rimasto ancorato all'opzione tradizionale, incentrata sul presupposto della capacità legale di agire, d'altra parte, il sistema accoglie e sviluppa al suo interno gli strumenti utili a consentire alla volontà del minore di trovare espressione[26].

L'art. 3, co. 1, l. 219/2017, stabilisce al riguardo che il minore ha diritto alla valorizzazione delle sue capacità di comprensione e decisionali, presupponendo la norma una legittimazione a decidere anche da parte della

---

obiettivi delle istituzioni scolastiche ai sensi dell'art. 1, co. 7, lett. h, l. 107/'15, legge sulla riforma nazionale del sistema di istruzione e formazione.

[24] M. SESTA, voce *Filiazione (diritto civile)*, in *Annali*, *Enc. dir.*, VIII, 2015, Milano.

[25] T. AULETTA, *Diritto di famiglia*, Torino, Giappichelli, 2016, 359 ss. e 367 ss., sul grado di discrezionalità e i limiti delle funzioni genitoriali.

[26] R. POTENZANO, *Il consenso informato, i trattamenti sanitari sui minori e decisioni di fine vita. Riflessioni comparatistiche*, in *Dir. fam. per.*, 2019, fasc. 3, 1307 ss., specie par. 3.

persona minore d'età.

Anche il codice di deontologia medica, pur riportando alla persona dei rappresentanti legali l'acquisizione del consenso, art. 37 co. 1, attribuisce significatività alle opinioni espresse dal minore, art. 35 ult. co., e impone al personale sanitario di segnalare all'autorità competente la sua opposizione verso un trattamento terapeutico ritenuto necessario quando il minore sia stato informato e ne sia stata accertata la capacità di comprensione, art. 37 co. 2.

I dubbi sui modelli disegnati dal legislatore, che si muove tra valorizzazione della capacità di discernimento dei minori e l'individuazione di una fascia d'età prefissata, non interessano esclusivamente le declinazioni civilistiche dell'ordinamento interno, ma coinvolgono anche i profili penalistici della tutela.

In quella sede, anche di recente, dottrina e giurisprudenza si sono confrontate sulla *ratio* operativa delle scelte normative, laddove in taluni casi si è inteso predeterminare il *finis* di partenza dal quale si riconosce generalmente nei minori l'idoneità a compiere scelte inerenti alla propria sfera intima, come nel caso del reato di cui all'art. 609 *quater* c.p. Diversamente per altri versanti connessi con la rappresentazione esterna della propria sessualità da parte del minore, ove la giurisprudenza ha faticato a comporre la necessità di punire invariabilmente determinate condotte illecite, in quanto idonee a coinvolgere minori d'età, e il riconoscimento in favore degli stessi minori di uno spazio sufficiente di autodeterminazione anche in una sfera delicata e peculiare[27].

3. Responsabilità genitoriale, diffusione dei dati personali dei minori d'età e tutele normative.

La responsabilità genitoriale, secondo la terminologia introdotta dalla novella sullo stato giuridico dei figli del 2012/2013, racchiude un complesso di funzioni, desumibili dalle norme codicistiche che intervengono sul contenuto e l'esercizio di tale situazione giuridica, di cui al tit. IX, capo I e II, libro I cod. civ., artt. 315 ss., ma anche dalle disposizioni che insistono sul sistema del tort e che modellano le responsabilità genitoriali in conseguenza dell'illecito dei figli minori, ex artt. 2047 e 2048 c.c.[28].

Il quadro è quello di un istituto complesso, in primo luogo sul piano soggettivo: tale funzione, infatti, investe non soltanto gli ascendenti diretti, ma anche coloro a cui eventualmente spettino i relativi compiti, quali sono, ad esempio, le famiglie affidatarie nell'ambito di un procedimento ove sia stato disposto l'affidamento familiare del minore, *ex* artt. 2 ss. l. 184/1983[29].

L'istituto della responsabilità genitoriale si presenta poliedrico anche sul

---

[27] S. BERNARDI, *La "pornografia domestica" davanti alle Sezioni Unite: alcune riflessioni sulla libertà del minore di disporre della propria immagine sessuale*, in *Riv. dir. proc. pen.*, 2022, fasc. 3, 1158-1187, nota a Cass. sez. un., 09.02.2022, n. 4616.

[28] G. FERRANDO, *La responsabilità per i danni prodotti dai minorenni*, in L. LENTI (a cura di), *Tutela civile del minore e diritto sociale della famiglia*, VI, Milano, 2002, 193 ss.

[29] Sul tema, A. MORACE PINELLI, *Note sparse intorno a una riforma del procedimento per l'affidamento dei minori*, in *Dir. fam. per.*, 2021, 1490-1504; per una precisazione sulle tipologie di affidamento eterofamiliare, Cass., 09.05.2024. n. 12717, in *De Jure*.

piano oggettivo e funzionale: i genitori sono tenuti all'adempimento dei doveri di cui all'art. 147 c.c., che rinvia all'art. 315 *bis* c.c., norma applicabile a tutte le declinazioni del rapporto di filiazione e che definisce un quadro che evita accuratamente il ricorso all'esercizio di situazioni di potere verso i figli minori, individuando nuovi termini per la descrizione di una relazione ove i genitori sono chiamati all'accudimento, all'educazione e al sostegno in modalità certamente più pervasive che in passato[30].

La nuova configurazione dei modelli genitoriali è stata accolta dalle corti, che hanno intrapreso un percorso di adeguamento al dettato normativo: ciò ha consentito di distinguere il legame tra gli adulti e quello sorto per effetto della filiazione, valutandosi positivamente la disponibilità dei genitori verso i figli pur in presenza di conflitti familiari[31].

Tra i presupposti che caratterizzano la condizione filiale, di cui all'art. 315 *bis* c.c., il dovere educativo è probabilmente quello che evoca connessioni con un più nutrito gruppo di profili d'indagine: i genitori sono infatti tenuti ad affiancare il minore nella crescita, curando il suo corretto inserimento nel contesto ambientale, off e on line. In questo spazio dovrebbero rientrare valori inclusivi, rivolti alla sfera familiare, scolastica e in generale tra pari, oltre che l'educazione alla valorizzazione della propria persona e alla condanna di condotte idonee a svilire o ledere la persona altrui.

Certamente si tratta di un incarico particolarmente gravoso, rispetto al quale dottrina e giurisprudenza[32] hanno segnalato evidenti difficoltà per gli esercenti la responsabilità genitoriale, dovute spesso all'assenza di strumenti di informazione, formazione e sostegno in favore degli adulti del complesso familiare[33].

Tra i pilastri che devono orientare le condotte genitoriali risiede l'obbligo di rispettare le inclinazioni e le aspirazioni dei figli, al fine di consentirne una corretta formazione in vista dell'evoluzione fisiologica della personalità e in attuazione del precetto di cui all'art. 30 Cost. (artt. 147, 315 *bis*, 316 c.c.): tale regola conserva la sua efficacia anche con riguardo a parental behaviours idonei a determinare un'impropria diffusione dei dati personali dei figli, in quanto trattasi di condotte potenzialmente escluse dall'esercizio di un reale potere di controllo da parte dell'interessato[34].

Come emerso in più occasioni[35], svariati sono i rischi connessi alla diffusione e condivisione on line da parte dei genitori dei dati personali identificativi dei figli: le condotte genitoriali sono infatti idonee a lasciare sul web tracce digitali che, recuperate in altre sedi, non soltanto possono configurare gravi forme di

---

[30] AA. VV., E*sercizio della responsabilità genitoriale*, a cura di S. PATTI-L. ROSSI CARLEO, Bologna, Zanichelli, 2021.
[31] Cass., 01.03.2023, n. 6186, in *De Jure*; v. sul tema, M. SESTA, *La prospettiva paidocentrica quale fil rouge dell'attuale disciplina giuridica della famiglia*, in *Fam. dir.*, 2021, 763-765.
[32] Cass., 10.09.2019, n. 22541, massima in *Resp. civ. prev.*, 2020, fasc. n. 2, 505.
[33] A. THIENE, *Gioventù bruciata on line: quale responsabilità per i genitori?*, in AA.VV., *Minori e privacy. La tutela dei dati personali dei bambini e degli adolescenti alla luce del regolamento (UE) 2016/679*, a cura di A. Annoni, A. Thiene, Napoli, 2019, 37-59; si legga pure il testo dell'art. 4 *bis*, l. 71/'17, introdotto di recente nell'ambito della normativa sul cyberbullismo dalla l. 70/'24, ove si prospetta il *favor* verso forme di supporto psicologico per gli studenti, includendo una previsione sul coinvolgimento delle famiglie.
[34] Trib. Roma, 23.12.2017, in *IUS* del 2 marzo 2018: nell'ambito di più ampio quadro di crisi familiare, l'ordine del giudice vieta a uno dei genitori di sovraesporre il figlio minore sui social, determinando la somma dovuta al tutore, nell'interesse del minore, in caso di mancata ottemperanza all'obbligo così definito.
[35] Trib. Trani, ord. 07.09.2021, con nota di G. Capilli, *La condivisione delle immagini di minori sui social network: quale tutela?*, in *Rivista di Internet*, 2022, 303 ss. V. pure Trib. Trani, 30.08.2021, in *De Jure*.

reato, ma anche dare luogo alla creazione di una personalità virtuale del minore che può non rispondere a quella nella quale lo stesso intende identificarsi, discostandosi da quella rappresentazione della propria persona che il minore è legittimato a rendere pubblica[36].

Ulteriore declinazione recente del fenomeno è quella connessa allo sharing di materiale digitale inerente a persone minori connotato dal conseguimento di profitti in favore delle figure genitoriali[37].

Tali questioni sono state discusse e affrontate in forma distinta dall'ordinamento francese, dapprima con l'approvazione della loi n. 1266 del 10 ottobre 2020, volta a inquadrare il fenomeno dello sfruttamento commerciale dell'immagine dei minori di sedici anni sulle piattaforme on line, seguita dalla loi n. 451 del 9 giugno 2023[38].

In seguito, il legislatore d'oltralpe ha introdotto modifiche al *code civil*, nel testo delle norme connesse all'autoritè parentale: la loi 2024-120 del 19 febbraio 2024, ha inserito all'art. 371-1, co. 2, il dovere dei genitori di proteggere la vita privata dei figli fino al conseguimento della maggiore età; all'art. 372 code civil, tra le disposizioni sull'esercizio dell'autorità parentale, si prevede che questa debba essere esercitata congiuntamente e, in questa direzione, la protezione della vita privata del figlio rappresenta un compito di cui entrambi i genitori sono incaricati, *ex* art. 372-1 co. 1 code civil, associandovi lo stesso figlio in considerazione dell'età e del grado di maturità, al co. 2 della norma citata.

Il concetto di vita privata, includendo anche doveri di garanzia a beneficio del minore avverso le condotte sia dei terzi sia di provenienza endofamiliare, è ricondotto dall'ordinamento nell'alveo dell'attuazione delle funzioni genitoriali, da cui anche le misure, essenzialmente interdittive e sanzionatorie, in caso di violazione, art. 373-2-6 co. 4 e 5 code civil, norma che disciplina l'intervento dell'autorità giudiziaria nelle questioni familiari.

Anche il legislatore interno ha avviato un percorso di riflessione sui temi illustrati: tra i progetti di legge presentati[39], nella proposta avviata alla Camera dei deputati per la prima lettura il 12 marzo 2024, A.C. 1771, e il cui esame in commissione è stato fissato a partire dal 26 giugno 2024, si conferma la volontà di regolare distintamente i due fenomeni, rappresentati, in un caso, dalla diffusione sulle piattaforme social delle performance riconducibili ai baby influencers e, nell'altro, dalla circolazione dei dati di soggetti minori per effetto essenzialmente delle scelte genitoriali, pur ponendosi l'accento sulla stretta

[36] E. BATTELLI, *Il trattamento dei dati nel prisma della tutela della persona minore d'età*, cit.; sul procedimento applicabile e sul contenuto delle disposizioni di cui agli artt. 473 *bis.38* e 473 *bis.39* c.p.c., norme introdotte dal d. lgs. 149/2022, in particolare sulle misure con funzione di tipo coercitivo, B. FICCARELLI, *Il nodo critico degli artt. 473-bis 38 e 473-bis 39 c.p.c.: riflessioni sul procedimento e una proposta interpretativa*, in *Judicium*, 11 marzo 2024, par. 2.1.

[37] *Relazione finale del Tavolo tecnico sulla tutela dei diritti dei minori nel contesto dei social networks, dei servizi e dei prodotti digitali in rete*, Roma, 10 maggio 2022, che si legge sul sito *garanteprivacy.it/temi/minori/sharenting*. Sul tema, I. GARACI, *The child's right to privacy in the family contest*, in questa *Rivista*, 2023, fasc. 1, 84-99.

[38] A. ROTA-M. VITALETTI, *La legge francese sugli influencer. Quale spazio per il diritto del lavoro?*, in *Law & Labor issues*, 2023, vol. 9, n. 2, 37-57.

[39] Oltre a quello a cui si accenna, i progetti di legge più recenti in materia sono AA.C. 1217, 1800, 1863: la documentazione può leggersi al seguente link: https://documenti.camera.it/leg19/dossier/Pdf/TR0109.pdf.

connessione tra i profili[40].

Con riguardo al primo, l'opzione normativa che il testo adotterebbe, contenuta all'art. 1, rinvia alle modifiche alla l. 977/1967, sulla regolamentazione del lavoro minorile, ove è stato riscritto in parte l'art. 4 e inserito un successivo art. 4 *bis*, che interviene espressamente sull'impiego dei minori sulle piattaforme digitali.

La nuova disposizione, art. 4 *bis*, al co. 6, richiama l'art. 2 l. 71/2017 tra gli strumenti di tutela: la norma consente al minore destinatario di atti di cyberbullismo e agli esercenti la responsabilità genitoriale di avanzare, verso il titolare del trattamento o gestore del sito, un'istanza per l'oscuramento, la rimozione ovvero il blocco dei dati personali della persona minore.

La novella attualmente in discussione approfondisce le misure di protezione già vigenti, ampliando l'ambito dei soggetti legittimati a promuovere l'istanza di rimozione dei contenuti indesiderati in caso di diffusione dei documenti multimediali afferenti al minore per ragioni di lucro e in violazione dell'obbligo di autorizzazione preventiva: ai soggetti già richiamati dalla normativa sui fenomeni del bullismo e cyberbullismo, la proposta di legge affianca anche i servizi sociali, le istituzioni scolastiche, l'autorità di pubblica sicurezza.

Di particolare interesse è il co. 7 dell'art. 4 *bis* che prevede, in caso di percezione di redditi superiori alla soglia definita da un successivo decreto, l'apertura di un conto corrente in favore del minore, gestito da un curatore speciale, con facoltà di accedere a una parte delle risorse patrimoniali a partire dal sedicesimo anno di età, in funzione del conseguimento d'interessi propri del minore. Tale indicazione risponde ad alcune delle criticità emerse nella presentazione della proposta di legge, tra cui anche un fenomeno emergente, qual è il mood genitoriale d'includere la prole minorenne nell'ambito della propria attività lavorativa e professionale on line, rafforzandosi, al tempo stesso, le misure di protezione in favore del minore nel senso d'impedire forme di sfruttamento per finalità estranee all'interesse della categoria[41].

Il fenomeno dello sharenting è affrontato all'art. 2, co. 1: il disegno di legge tutela espressamente il diritto alla riservatezza dei minori, in attuazione di quanto previsto dalla Carta di Treviso, come modificata nel 2021 in funzione protettiva e preventiva; si pone, inoltre, un divieto generalizzato che ha per oggetto la diffusione di notizie/contenuti multimediali inerenti al minore e grava in modalità indifferenziata su tutti i terzi, con il limite dell'interesse della persona coinvolta.

La disposizione contiene un riferimento alla diversificazione delle condizioni in cui i minori possono trovarsi in ragione dell'età: è previsto, infatti, un espresso rinvio al "regolare processo di maturazione" del minore, che potrebbe essere alterato dalla diffusione di dati personali a lui inerenti.

Al co. 2, su imitazione della legge francese, si attribuisce ai genitori l'esercizio congiunto della tutela dell'immagine del figlio, associandovi anche i discendenti, alla luce dell'età e del grado di maturità: la norma, infatti, pone a

[40] La proposta può leggersi al seguente link: *https://documenti.camera.it/leg19/pdl/pdf/leg.19.pdl.camera.1771.19PDL0081550.pdf*.

[41] "Lo sharenting è un fenomeno da tempo all'attenzione del Garante, soprattutto per i rischi che comporta sull'identità digitale del minore e quindi sulla corretta formazione della sua personalità. La diffusione non condivisa di immagini rischia inoltre di creare tensioni anche importanti nel rapporto tra genitori e figli.": dal sito *www.garanteprivacy.it*.

carico dei genitori il dovere di coinvolgere la prole minorenne, mediante l'uso di una terminologia nuova nell'ambito delle situazioni in cui si prospetta l'esercizio di un diritto del minore di natura personale.

Non del tutto aderente alle indicazioni precedenti appare la qualificazione normativa della decisione genitoriale di pubblicare dati inerenti all'immagine della prole, notizie/informazioni/contenuti multimediali quale atto di straordinaria amministrazione, richiamandosi gli artt. 147 e 357 sulle funzioni del tutore (co. 3): sul punto, maggiore linearità sarebbe affiorata dal rinvio all'art. 316 co. 1 c.c., sull'esercizio della responsabilità genitoriale in comune accordo tra gli ascendenti, secondo le indicazioni provenienti anche dalle corti[42].

Ulteriori dubbi sulla compatibilità con le indicazioni che si traggono dalla prima parte della disposizione, art. 2 co. 2, sorgono anche per effetto del rinvio, operato dalla stessa previsione, (anche) all'art. 320 c.c.: come noto, la norma codicistica opera essenzialmente per gli atti di straordinaria amministrazione, subordinandoli, al co. 3, alla ricorrenza di necessità e utilità evidenti in favore del figlio e previa autorizzazione dell'autorità giudiziaria[43].

Ancora, oggetto di richiamo in funzione di tutela è anche la normativa sul cyberbullismo: all'art. 2, co. 4, si consente al minore quattordicenne di richiedere direttamente la cancellazione dei dati, anche con riguardo ai contenuti diffusi dagli esercenti la responsabilità genitoriale.

Per quanto attiene all'inquadramento generale delle nuove previsioni, il legislatore interno pare rinunciare all'inserimento delle norme nel testo della disciplina codicistica sulla responsabilità genitoriale, riservandosi un intervento di legislazione speciale, sia pure declinando la tutela dell'immagine e della riservatezza del figlio all'interno dell'esercizio delle funzioni tipicamente genitoriali (art. 2 co. 2 e 3).

L'opzione adottata appare conforme alle indicazioni codicistiche, oltre a essere modellata su quanto previsto dalle disposizioni sul consenso ai trattamenti sanitari, in quanto si consentirebbe ai genitori di adottare le decisioni inerenti al diritto all'immagine dei figli (art. 2 co. 3), predisponendo in favore del minore il potere di prendere parte al processo decisionale in considerazione dell'età e della maturità (co. 2).

Le disposizioni citate sarebbero indicative di un processo che non soltanto vira in direzione di una maggiore protezione dei minori, ma disegna allo stesso tempo un quadro ove i rischi derivanti ai minori dall'uso dei dispositivi digitali paiono prevalere sui benefici.

Tale lettura sembrerebbe confermata dall'art. 4 del disegno di legge: l'intervento normativo si propone infatti di posticipare l'età prevista dall'art. 2 *quinquies* d. lgs. 196/2003, spostando la soglia utile a manifestare il consenso al trattamento dei dati da quattordici a sedici anni, soluzione che confermerebbe il ruolo degli esercenti la responsabilità genitoriale sul tema[44].

---

[42] Trib. Rieti, 07.03.2019, in *ilfamiliarista.it* del 16 luglio 2019, con nota di S. Alessandro: si conferma la regola del consenso prestato da parte di entrambi i genitori in funzione della pubblicazione sui social di contenuti inerenti ai figli minori.

[43] Sul tema, G. CARAPEZZA FIGLIA, *Sharenting: nuovi conflitti familiari e rimedi civili*, in *Nuova giur. civ. comm.*, 2023, I, 1104-1108, commento a Trib. Rieti, 17.10.2022, n. 443, ivi, 1108-1111, e giurisprudenza citata.

[44] L'innalzamento della soglia d'età per la prestazione del consenso al trattamento dei dati, anche se a quindici anni, è stato previsto anche dal progetto di legge A.C. 1217, art. 1 co. 1, mentre al co. 3 sono

Resterebbero ferme le misure ordinarie esperibili nell'ambito della relazione genitoriale a garanzia dell'interesse del minore: sul punto, la riforma del processo civile non ha escluso l'estensibilità ad ulteriori figure, anche estranee all'ambito familiare, di talune funzioni di rappresentanza e assistenza della persona incapace, di natura processuale, ma anche di tipo sostanziale. Tra queste, rileva in particolare la funzione del curatore speciale, come modellata dal novellato art. 78 c.p.c. e dall'art. 473 *bis.*8 c.p.c., istituto a cui si rinvia anche in caso di affidamento del minore ai servizi sociali, *ex* art. 5 *bis* l. 184/1983, norma introdotta nel testo della normativa sull'affidamento familiare dal d. lgs. 149/2022[45].

Affiorano, inoltre, i dubbi prospettati dalla dottrina sulle competenze genitoriali in ordine alla vigilanza sull'uso e la gestione dei tools digitali da parte dei minori: ciò da un lato confermerebbe il ruolo essenziale proprio della funzione educativa degli adulti di riferimento. D'altra parte, la configurazione dell'istituto della responsabilità genitoriale sarebbe decisamente more deep, richiedendosi ai genitori non soltanto di affiancare il figlio nella propria naturale evoluzione psico-sociale, ma anche di acquisire expertises oggetto di un costante aggiornamento[46].

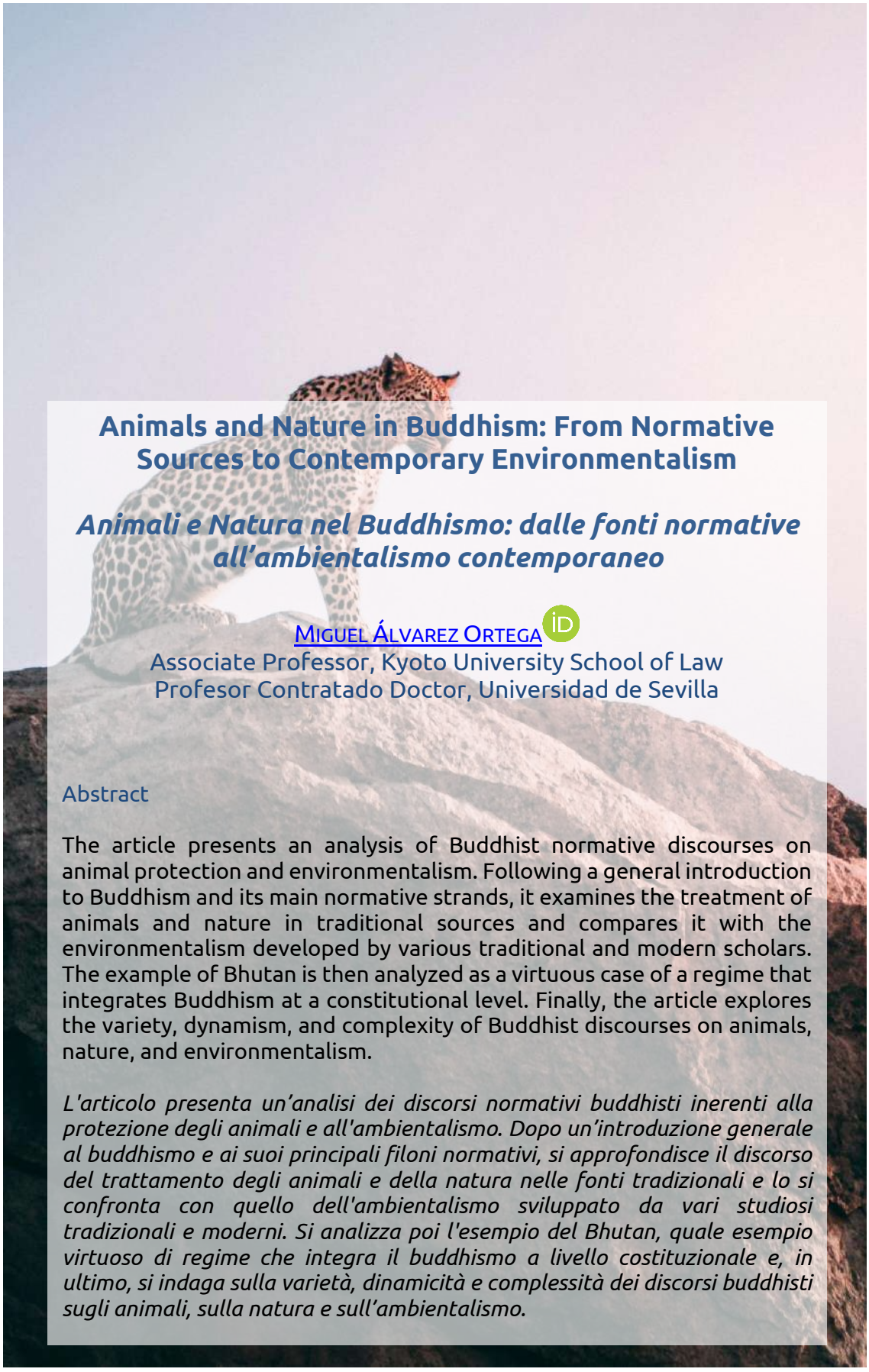
disposte norme più stringenti per la verifica dell'età dei minori che richiedono l'accesso ai servizi. Un ulteriore progetto in materia, A.C. 1863, all'art. 3, stabilisce la nullità dei contratti stipulati tra le società che forniscono servizi digitali e i minori di anni quindici e propone l'abrogazione delle disposizioni attualmente vigenti nel territorio sulla soglia utile a prestare il consenso digitale, conservandosi come fonte di riferimento in materia quanto previsto dal regolamento del 2016 (art. 4).

[45] Sull'intervento normativo v. in senso dubitativo A. Thiene, *Dalla parte delle famiglie per un diritto minorile gentile*, *op. cit.*, specie 1320 ss.; si legga pure Cass. civ., 15.01.2024, n. 1390, in *De Jure*, che ha rimesso dinanzi alle sezioni unite la questione relativa alle conseguenze dell'omessa nomina del curatore speciale nell'ambito di un giudizio sull'adozione c.d. mite.

[46] Sul sostegno e la formazione parentale nell'ambito dei procedimenti di alfabetizzazione digitale, v. pure, art. 14 co. 1 d.l. 123/'23; A.R. Popoli, *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, op. cit., 1309, sull'inidoneità genitoriale a vigilare in particolare sulle privacy policies.

Álvarez Ortega M, 'Animals and Nature in Buddhism: From Normative Sources to Contemporary Environmentalism' (2024) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT242MAO

EJPLT
ISSN 2704-8012



Animals and Nature in Buddhism: From Normative Sources to Contemporary Environmentalism

Animali e Natura nel Buddhismo: dalle fonti normative all'ambientalismo contemporaneo

MIGUEL ÁLVAREZ ORTEGA
Associate Professor, Kyoto University School of Law
Profesor Contratado Doctor, Universidad de Sevilla

Abstract

The article presents an analysis of Buddhist normative discourses on animal protection and environmentalism. Following a general introduction to Buddhism and its main normative strands, it examines the treatment of animals and nature in traditional sources and compares it with the environmentalism developed by various traditional and modern scholars. The example of Bhutan is then analyzed as a virtuous case of a regime that integrates Buddhism at a constitutional level. Finally, the article explores the variety, dynamism, and complexity of Buddhist discourses on animals, nature, and environmentalism.

L'articolo presenta un'analisi dei discorsi normativi buddhisti inerenti alla protezione degli animali e all'ambientalismo. Dopo un'introduzione generale al buddhismo e ai suoi principali filoni normativi, si approfondisce il discorso del trattamento degli animali e della natura nelle fonti tradizionali e lo si confronta con quello dell'ambientalismo sviluppato da vari studiosi tradizionali e moderni. Si analizza poi l'esempio del Bhutan, quale esempio virtuoso di regime che integra il buddhismo a livello costituzionale e, in ultimo, si indaga sulla varietà, dinamicità e complessità dei discorsi buddhisti sugli animali, sulla natura e sull'ambientalismo.

© The author(s) 2024, 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: Buddhism; animals; nature; environmentalism

Summary: 1. Introduction. – 2. Buddhism: Western reception, history, and features. – 3. Normative Spheres in Buddhism. – 4. Animals and Nature in Buddhist Normative Sources. – 5. Animals and Environmentalism in Contemporary Buddhist Scholarship. – 6. An Implementation Case: The Kingdom of Bhutan. – 7. Concluding remarks.

1. Introduction.

This paper presents an approach to Buddhist normative discourses on animal protection and environmentalism. To do so, I will first introduce Buddhism as a tradition, dealing with its main features, history, and reception in the West (2) and providing a comprehensive account of its different normative strands (3). This will allow us to tackle the specific treatment of animals and nature in traditional sources (4) and compare it with the discourses on environmentalism presently developed by both traditional and modern scholars (5). The country of Bhutan will be addressed as an example of a regime which embraces Buddhism at the constitutional level and has been internationally recognised for its environmental agenda and accomplishments (6).

The concluding thesis I would like to explore is that, in contrast to simplifying and essentialising idealisations, Buddhist discourses on animals, nature, and environmentalism constitute a complex and rich tapestry prompted by diversity, internal and external tensions, and potentialities (7).

2. Buddhism: Western reception, history, and features.

From the affable, televised image of the Dalai Lama to the evocative references of beat generation writers to a wide range of commercial uses of iconographic elements in chill-out venues and New Age paraphernalia, Buddhism is not just a part but a significant contributor to the popular culture of the globalised world. Its influence is felt across continents and cultures. This globalised nature of Buddhism is a relatively recent development. While contact between the West and Buddhist traditions can be traced back to the ancient world, it was markedly partial, unsystematic, and discontinuous until the nineteenth century. The Greek-Buddhist interface of Gandara (), responsible for the Hellenistic-inspired sculptures of a Buddha in robes and a hair bun, did not result in a Western spread of his teachings.[1] At the same time, the missionary enterprise carried out between the sixteenth and eighteenth centuries in Asia, especially by the Portuguese and Spanish, would form a new context of rapprochement, although in general, it would not generate either a

[1] See J Boardman, *The Diffusion of Classical Art in Antiquity*, vol 42 (Princeton University Press 2023) 109-144; DS Lopez (ed.), *Critical Terms for the Study of Buddhism* (The University of Chicago Press 2005) 26-27.

popularization of the religion in Europe or a weighty academic corpus, mainly due to a lack of capacity to read and study the texts.[2]

By the mid-19th century, the Western colonial presence in Asia enabled and prompted a multilateral absorption of Buddhism. This reception was undertaken by a diverse group of scholars and thinkers, including philologists and historians of religions, like E. Burnouf and T.W. Rhys Davids;[3] Modernist spiritualists, like P. Carus and D. T. Suzuki; [4] and German intellectuals like Schopenhauer and Nietzsche.[5] This complex scenario allowed the formation of a scholarly corpus dedicated to Buddhist notions and sources, as well as a matrix for a practical approach to the tradition as an allegedly non-religious and scientific spirituality. Thus, today, we find a rich tapestry of exposures and approaches to Buddhism as a specialized academic field of study, a religious and spiritual practice (with both traditional and modern takes), and the object of interest of global pop culture, from famous actors to clothing merchandising.

Despite this seeming familiarity, Buddhism is still not typically part of the regular Western educational background, so it may be worth providing a contextualising description, which may be skipped by those already versed in the tradition. Under the generic label of 'Buddhism,' there is a set of religious and philosophical traditions that extend throughout much of Asia, from Sri Lanka to Japan, through the Himalayas and Southeast Asia. The common origin of these traditions is found in the teachings imparted in North India by Siddhārta Gautama (Pāli: Siddhattha Gotama) between the 5th and 4th centuries B.C.[6]

According to tradition, Siddhārta belonged to a ruling family of the Śākya republic. After experiencing the dissatisfactions and displeasures of a hedonistic and materialistic life, at the age of 30, he decided to undertake a path of extreme renunciation in which he also did not find an answer to his concerns. Finally, during a session of spiritual practice in which he seeks a balance or middle ground between self-indulgence and self-mortification, he reaches the state of enlightenment known as *nibbana* (Pāli) or nirvana (Westernization of the Sanskrit *nirvāṇa*), ceasing his suffering and attaining wisdom. He thus becomes the Buddha, literally, 'the one who has awakened.[7] And so begins a process of propagation of his teachings, of his discovered

---

[2] According to Urs App, the first contact with Buddhist texts would not take place in India but in 16th century Japan, while the first sūtra translated into a European language would be the Chinese version of the Sūtra of the 42 Sections (四十二章經, sì shí èr zhāng jīng). U App, *The Birth of Orientalism* (University of Pennsylvania Press 2011) 8-9.

[3] E Bender, JW de Jong, 'A Brief History of Buddhist Studies in Europe and America' (1978) 98 Journal of the American Oriental Society 350, 40 ff.; J Snodgrass, 'Defining Modern Buddhism: Mr. and Mrs. Rhys Davids and the Pāli Text Society' (2007) 27 Comparative Studies of South Asia, Africa and the Middle East 186, 186–202.

[4] DL McMahan, *The Making of Buddhist Modernism* (Oxford University Press 2008) 93–102; DL McMahan, 'Modernity and the Early Discourse of Scientific Buddhism' 72 897, 909 ff.

[5] P Abelsen, 'Schopenhauer and Buddhism' (1993) 43 Philosophy East and West 255, 255–278; BA Elman, 'Nietzsche and Buddhism' (1983) 44 Journal of the History of Ideas 671, 680 ff.

[6] On the issue of dating the Buddha, see LS Cousins, 'The Dating of the Historical Buddha: A Review Article' (1996) 6 Journal of the Royal Asiatic society 57, 57–63; HW Schumann, *The Historical Buddha: The Times, Life, and Teachings of the Founder of Buddhism*, vol 51 (Motilal Banarsidass Publ 2004).

[7] For the traditional account, see C Willemen and Numata center for Buddhist translation and research staff, *Buddhacarita: In Praise of Buddha's Acts: (Taishō Volume 4, Number 192)* (Calif: Numata Center for Buddhist Translation and Research 2009).

truths, known as 'Buddha-dharma' or simply 'Dharma,' a comprehensive Indian term. Buddhism is thus constructed in dialogue with the Hindu schools and, despite the secularising characterisations seen today (scientific spirituality) and the complexity of the elements it contains, it is still a 'religion': It admits the Hindu pantheon of deities, attributes supernatural properties to the Buddha and the enlightened beings, believes in reincarnation in six different worlds (including that of demons and hungry ghosts), and develops a monastic body whose functions include the practice of rituals.[8]

The first teaching of Siddhārtha contains the fundamental principles of the Buddhist path and is identified with the 'four noble truths' that focus on the experience of suffering (*dukkha*) as a part of human life.[9] The notion of 'suffering' employed encompasses a wide variety of manifestations-from physical pain to deprivation of objects of desire are caused by thirsty craving (*taṇhā*) conditioned by ignorance (*avijjā*), which manifests as emotional attachment (*lobha, rāga*), hatred or aversion (*dosa*) and mental obfuscation (*moha*). It is thus intended to point out that people crave or detest things due to a lack of understanding of the vacuous (suñña), dynamic, and interrelated nature of all objects and beings (*paṭiccasamuppāda*), including human beings themselves, so that the person is regarded as a dynamic and plural set of elements known as *anattā* (absence of essential soul).[10] This has led some authors to mistakenly identify a kind of nihilism that denies the individual.[11] Actually, it is generally understood that the purpose of Buddhism is not to deny the existence of the moral agent, but to present a multifactorial and dynamic image of the person as a set of interrelated elements (*kandhas*), as opposed to the essentialist and static conception common in Brahmanical thought.[12]

To put an end to suffering, it is necessary to put an end to the state of ignorance described above, which implies attaining *nibbana* (nirvana). This notion, initially taken in the West as synonymous with annihilation or even cessation of existence, implies a specific way of being in the world and, as a spiritual goal, involves ending the cycle of reincarnations in the conditioned world, the saṃsāra. Nirvana and samsara are thus two opposite ways of experiencing reality. To attain Nibbana, the Buddha describes a set of nuclear practices known as *magga*, the Buddhist eightfold path.[13]

These notions constitute a sort of shared core that will be historically developed in a plurality of sources and traditions as Buddhism expands throughout much of Asia. From certain current conventions, and following what are traditionally called 'turns of the dharma wheel,' a tripartite division is

---

[8] M Southwold, 'Buddhism and the Definition of Religion' (1978] Man 362, 362–379.

[9] MV Ram Kumar Ratnam, *Dukkha: Suffering in Early Buddhism* (Discovery Publishing House 2003); C Anderson, *Pain and Its Ending: The Four Noble Truths in the Theravada Buddhist Canon* (Routledge 2013).

[10] See, among many others, A Wayman, *Dependent Origination: The Indo-Tibetan Tradition* (Reidel 1980); JL Garfield, 'Dependent Arising and the Emptiness of Emptiness: Why Did Nāgārjuna Start with Causation?' (1994] Philosophy East and West 219.

[11] WH Burns, *The Doctrine of 'Anatman' in Early Buddhism* (The University of Texas at Austin 1991).

[12] R Gethin, 'The Five Khandhas: Their Treatment in the Nikāyas and Early Abhidhamma' (1986) 14 Journal of Indian Philosophy.

[13] The eightfold noble path (*ariya aṭṭhaṅgika magga*) breaks down into: 1. Right view; 2. Right intentionality; 3. Right speech; 4. Right action; 5. Right way of life; 6. Right effort; 7. Right mindfulness and awareness; 8. Right samādhi. For a clear and accessible explanation, see W Rahula, *What the Buddha Taught* (Open Road+ Grove/Atlantic 2007) ch V.

usually presented, which would include: the Theravāda tradition or doctrine of the ancients (considered the most archaic and prevalent in Sri Lanka and Southeast Asia);[14] the great vehicle or Mahāyāna tradition developed from the beginning of the Christian era and spreading to North and East Asia, centred on the model of the bodhisattva (Pāli: bodhisatta), who seeks the salvation of all sentient beings;[15] and tantric Buddhism, way of the diamond or Vajrayāna (part of the Mahāyāna tradition centred on esoteric methods, whose major representative is Tibetan Buddhism). [16] The three vehicles would appear historically in succession and have their own canonical collections, known as Tipiṭakas (or Tripiṭakas; lit. 'the three baskets') because of their tripartite division into discourses (suttas, sūtras), monastic discipline (Vinaya)and epistemological and ontological elaborations (Abhidhamma,Abhidharma). Although the oldest preserved texts are in the Gāndhārī language, [17] the primary canonical corpus is identified in the impressive collection of the Canon Pāḷi, of the Theravāda tradition, of which the Pāli Text Society edition consists of 57 volumes.[18]

In terms of public space, the influence of Buddhism varied considerably according to location and time. In India, after achieving transcendent momentum during the reign of Aśoka (268-232 B.C.), it would later be pushed aside by other local traditions and driven into virtual irrelevance after the Mughal invasion;[19] however, it has continued to have a strong foothold in Sri Lanka to this day. [20] Regarding Southeast Asia and the Himalayas, Andrew Huxley has pointed out that Buddhism arrived as part of a civilizing and enlightening pack with no equivalent local competitors, which explains its unavoidable cultural centrality at all levels.[21] Thailand, Burma, and Tibet are clear examples. On the other hand, in the case of the Sinosphere, which already had its own philosophical and religious background, Buddhism would come into play in a competitive scenario, and its influence would necessarily be diverse and, at times, more peripheral. This has not prevented, for example, a secular country with a Confucian substratum, such as Japan, from having a Buddhist party with a parliamentary presence.[22]

Today, Buddhism is a global tradition with almost 500 million followers, almost half of whom are in China, and it is the majority religion in Cambodia, Thailand (where it exceeds 90%), Burma, Bhutan, Sri Lanka, Laos, and

[14] R Gombrich, *Theravada Buddhism A Social History from Ancient Benares to Modern Colombo* (Routledge 2006); K Crosby, *Theravada Buddhism: Continuity, Diversity, and Identity* (John Wiley & Sons 2013).
[15] P Williams, *Mahāyāna Buddhism: The Doctrinal Foundations* (2nd edn., Routledge Taylor & Francis Group 2009).
[16] RM Davidson, *Indian Esoteric Buddhism. A Social History of the Tantric Movement* (Columbia University Press 2003); CK Wedemeyer, *Making Sense of Tantric Buddhism: History, Semiology, and Transgression in the Indian Traditions* (Columbia University Press 2014).
[17] E Fumio, 'The Discovery of 'the Oldest Buddhist Manuscripts'' (2000) 32 The Eastern Buddhist 157.
[18] S Collins, 'On the Very Idea of the Pali Canon' (2005) 8 Buddhism: Critical Concepts in Religious Studies 72.
[19] KTS Sarao, *The Decline of Buddhism in India: A Fresh Perspective* (Munshiram Manoharlal Publishers 2012).
[20] HR Perera, *Buddhism in Sri Lanka: A Short History* (Buddhist Publication Society 1988).
[21] A Huxley, 'How Buddhist Is Theravāda Buddhist Law?: A Survey of Legal Literature in Pāli-Land', *The Buddhist Forum* (The Institute of Buddhist Studies 1990) 42.
[22] A Palmer, *Buddhist Politics: Japan's Clean Government Party* (Springer Science & Business Media 2012).

Mongolia.[23] It is also undeniable that Buddhism has been long experiencing a clear boom in the West, especially among the educated upper-middle classes of the left.[24]

3. Normative Spheres in Buddhism.

One of the most deeply rooted beliefs in the West regarding Buddhism relates to an alleged renunciation of life in the world that would make it a religion unconcerned with society, politics, and norms. This notion, abandoned in contemporary specialist circles, was once supported by important figures of thought, such as Max Weber or Ortega y Gasset.[25] While it is true that Buddhist soteriology focuses on individual praxis and that the bulk of its literature and philosophy is concerned with questions of an epistemological or religious nature, this does not imply the development of a normative fabric of its own, which will be classified here as: a. Generic and secular ethics, b. Kingship models, c. Monastic regulation, and d. Buddhism-inspired law.

a. *General and secular ethics*.

General morality comes into play as an essential part of the path to clear out the afflictive emotions that impede realization – ignorance, grasping, and aversion. Thus, *śīla*, i.e. Ethics, constitutes one of the spheres of cultivation along with *samadhi* (meditative concentration) and *prajña* (wisdom) within the Octuple Noble Path.[26] General morality appears as a set of requirements for the agents. The basic standard for laypeople is known as the 'five precepts' (*pañca-sīlāni*) and strongly resembles the commands stated in major religions and traditions. It is usually recited as part of a formula of spiritual adherence to the Buddhist practice known as 'taking refuge,' in which practitioners undertake the precepts to refrain from destroying living creatures, taking that which is not given, sexual misconduct, incorrect speech and intoxicating drinks and drugs which lead to carelessness.

The existence of longer lists of precepts, along with varied contextual ethical angles and considerations, has allowed Peter Harvey to refer to 'gradualism' as a defining feature of Buddhist morality, which tries to adapt its content to the capacities and commitment of the practitioner.[27] As for the elements that build up moral judgment, according to Vélez de Cea: 'Early Buddhist ethics […] tends to integrate in its criteria of goodness three factors: motivation and content of actions (wholesomeness, blamelessness) and their consequences (harmless and happy results for oneself and others).[28]

---

[23] C Hackett, BJ Grim, 'Buddhists', *The Global Religious Landscape: A Report on the Size and Distribution of the World's Major Religious Groups as of 2010* (Pew Research Center) 31-34.
[24] JW Coleman, *The New Buddhism: The Western Transformation of an Ancient Tradition* (1st edn, Oxford University Press USA 2001).
[25] M Weber, *Economy and Society. An Outline of Interpretive Sociology* (Univ of California Press 1978) 504, 546; J Ortega y Gasset, 'Ensimismamiento y Alteración: Meditación de La Técnica', *Obras Completas. Tomo V (1932-1940)* (Taurus 2006) 579.
[26] D Keown, *The Nature Buddhist Ethics* (Palgrave 2001) 108–109.
[27] P Harvey, *An Introduction to Buddhist Ethics* (Cambridge University Press 2000) 51 ff.
[28] A Vélez de Cea, 'The Criteria of Goodness in the Pali Nikayas and the Nature of Buddhist Ethics' (2004) 11 Journal of Buddhist Ethics 123, 139.

In the case of the Mahāyāna traditions, in general, it is understood that morality takes on an all-encompassing role in the Buddhist soteriological project and expands to encompass temperance, the cultivation of virtues and moral skills, and altruism or the intention to benefit all sentient beings.61 In this way, compassion (*karuṇā*) is considered the true guiding value. At the same time, the texts offer a sort of list of 'new' precepts, known as *śikṣāpadas*, in which exceptional and contextual transgressions are accommodated under the complex notion of *upāya-kauśalya* (skillful means).[29] The model here is that of the bodhisattva, who, despite his spiritual realization, decides to remain in saṃsāra to help liberate all beings. In general, compared to the Pāli sources, the ethical developments of the Mahāyāna traditions are characterized by a greater emphasis on empathy and altruism -and thus greater social involvement- as well as by allowing for less rigid and more complex moral reasoning.

On the other hand, it is notable that academic interest in Buddhist Ethics, beyond the philosophical disquisitions on the proper way to classify it,[30] has grown exponentially in recent years, focusing on problems of normative ethics, mainly in the environmental, health, and social welfare fields.[31]

b. *Kingship models.*

In Buddhist sources, the treatment of power is plural, complex, and sometimes contradictory, particularly concerning the exercise of punishment and violence,[32] and often revolves around exemplary figures of monarchs. Thus, we find the model of the consensual monarch (*Mahāsammata*), mythically chosen to guarantee respect for the crops of others;[33] the model of the universal monarch (*Cakkavattin*) who conquers and governs the ends of the world peacefully;[34] or the model of the messianic monarch (*Metteya*), who would appear as the Buddha of the future to put an end to an era of dismal human decadence.[35] In any case, the prevailing and largely overlapping model is that of the virtuous monarch who rules according to Buddhist principles (Dhammarāja), so that the specific treatment of governance tends to be framed

[29] Keown (n 26) 145.

[30] Utilitarianism (avoidance of suffering), eudemonism (cultivation of virtues), and complex contextualism (motivation, skills, means, effects), among others, have been used as labels to describe Buddhist Ethics.

[31] Among many other examples, see C K Tucker and D William, *Buddhism and Ecology: The Interconnection of Dharma and Deeds (Religions of the World and Ecology)* (Center for the Study of World Religions 1997); B. Mettanando, 'A Buddhist Model for Health Care Reform' (2007) 90 J Med Assoc Thai 2213; P Sahni, *Environmental Ethics in Buddhism: A Virtues Approach* (Routledge, Taylor & Francis Group 2008); SP James, *Zen Buddhism and Environmental Ethics* (Routledge 2017); J Magnuson, *From Greed to Wellbeing: A Buddhist Approach to Resolving Our Economic and Financial Crises* (Policy Press 2016); D Keown, *Buddhism and Bioethics* (15th ed, Palgrave Macmillan Limited 2016); P De Silva, *Environmental Philosophy and Ethics in Buddhism* (Springer 2016).

[32] M Zimmermann, 'Only a Fool Becomes a King: Buddhist Stances on Punishment' in M Zimmermann (ed.), *Buddhism and Violence* (Publications of the Lumbini International Research Institute 2006) esp. 220-221.

[33] See the opposing takes of RS Sharma, *Aspects of Political Ideas and Institutions in Ancient India* (4th rev. ed, Motilal Banarsidass Publishers 1996) 49 ff; S Collins, 'Discourse on What Is Primary (Aggañña-Sutta)' (1993) 21 Journal of Indian Philosophy 301, 317.

[34] See GT Halkias, 'The Enlightened Sovereign' in SM Emmanuel (ed.), *A Companion to Buddhist Philosophy* (John Wiley & Sons 2014) 498 ff.

[35] See the collective and comprehensive volume A Sponberg, H Hardacre, *Maitreya, the Future Buddha* (Cambridge University Press 1988).

in terms of the virtues, attitudes, and prudential policies that characterise a moral king.

In general, the following of Dharma imposes on the ruler a series of duties and measures centred around creating the conditions of social order.[36] Specific approaches to this model can be found in the *Jātakas*, accounts of the Buddha's past lives, where the qualities of the *dhammarāja*, including generosity, nonviolence, or justice as the cause of well-being and happiness, are recounted.[37] Sometimes, such narratives explain how the presence of a just king not only leads to the good behaviour of the subjects and makes violence unnecessary but also causes prosperity to flourish in the kingdom or fruits to grow juicy and sweet on the trees, which shows the ontological nuances of dharma.[38] These kinds of ideal qualities serve, it has been pointed out, to attempt to circumvent the problem of potentially unnecessary coercion and its possible karmic consequences [39] and find their counterpart in other descriptions of the model king in which pragmatism prevails and various applications of force by the ruler are permitted, including even capital punishment. [40] For example, the Mahāyāna sutra *Ārya-Bodhisattva-Gocara* contains concrete instructions on the government where the problems of criminal law and the art of war are dealt with extensively from a practical perspective, but always avoiding cruelty in the former and considering the latter as the ultima ratio.[41]

c. *Monastic regulation*

Buddhism's primary and most relevant normative expression is usually located in the monastic regulations, codified as Vinaya, one of the three parts, as seen above, of the Buddhist canons. Derived explicitly or implicitly from the Buddha himself, its typical structure involves a twofold division known as the *Vibhang*a, whose regulative core is called the *Pāṭimokkha* (Sanskrit: *Prātimokṣa*), and the *Kandhakas*, which contain the communal acts performed by the

[36] These measures are usually of a material and welfare nature and are related to the foreseeable consequences of neglecting the duty of care, connected with conditional arising (*paṭiccasamuppāda*, *pratītyasamutpāda*). Thus: 14. ´In this way, monks, money not being given to the poor, poverty flourished; because poverty flourished, theft flourished; because theft flourished, weaponry flourished; because weaponry flourished, murder flourished; because murder flourished, these beings' vitality decreased, as did their beauty; because their vitality and beauty decreased, those who lived for eighty thousand years had children who lived for (only) forty thousand» (…). S Collins, '3 - The Discourse (Containing) a Lion's Roar on the Wheel-Turning King (Cakkavatti-Shanda Sutta)' (1998) 608.

[37] The ten real virtues (*Dasa-rājādhamma*) are: generosity (*dāna*), morality (*sīla*), sacrifice (*pariccāga*), honesty (*ajjava*), temperance (*madddava*), self-control (*tapa*), non-rage (*akkodha*), non-violence (*ahimsā*), patience (*khanti*) and tolerance (*avirodha*). S Collins, 'Recipes for a Good King: Ten Virtues, Four Wrong Courses, Four Forms of Kindliness, Five Precepts', *Nirvana and Other Buddhist Felicities: Utopias of the Pāli Imaginaire* (Cambridge University Press) 460 ff.

[38] Sensu contrario, if the king does not behave properly, misfortunes occur. BG Gokhale, 'The Early Buddhist View of the State' (1969) 89 Journal of the American Oriental Society 731, 736; BG Gokhale, 'Early Buddhist Kingship' (1966) 26 The Journal of Asian Studies 15, 20.

[39] Collins (n 36) 442.

[40] BG Gokhale, 'The Early Buddhist View of the State' (1969) 89 Journal of the American Oriental Society 731, 735.

[41] L Jamspal, PG Hackett, *The Range of the Bodhisattva, A Mahāyāna Sūtra (Ārya-Bodhisattva-Gocara): The Teachings of the Nirgrantha Satyaka* (The American Institute of Buddhist Studies : Columbia University's Center for Buddhist Studies : Tibet House US 2010) 47–63.

monastic community (*saṅgha*).[42] If we turn, for example, to the *Pāṭimokkha* Theravadin, we find 227 rules (for monks) covering a wide range of topics varying from essential problems for coexistence, such as homicide or the provocation of schisms, to minor issues, such as the making of habits. The rules are organised into eight sections according mainly to the sanction envisaged, which may consist of the need for confession, being made available or various degrees of ostracism.[43] The Vinaya has its own normative characteristics derived from both Buddhist philosophy and its peculiar addressees, which explain the marginality of the coercive use of force.[44] Specialists also allude to a desire for flexibility and contextual adaptation, given, among other reasons, that the Buddha himself was not only casuistic in his normative elaboration but also applied and justified exceptions and modulations for concrete cases.[45] On the other hand, one should not lose sight of the complex nature of the Vinaya, which includes both elements of training, so to speak, for the monks, along with matters of greater normative orthodoxy;[46] while the need to contextualise and not idealise its effective use in monasteries, which usually have specific internal organisational regulations, has been stressed by different scholars.[47]

d. *Buddhism-inspired Law.*

To what extent it is accurate to speak of a Buddhist legal genre in a secular, secular or generalist sense is a complex and debated question, marked naturally by the sphere of meaning attributed to Buddhism, law, and the relations between the two. Not surprisingly, the area of expertise devoted to these issues has tended to opt for the flexible and open-ended label of 'Buddhism and Law', reserving 'Buddhist Law' for Ecclesiastical or Monastic regulations.[48] If we descend to context-specific studies, in the case of South Asia, the tradition states that Aśoka converted to Buddhism after the atrocities of the Kalinga War and decided to promote and rule according to the Buddhist dharma, his edicts being considered a normative expression of these aims.[49]

In the case of Sri Lanka, Buddhism has had a continuous and relevant influence from the third century B.C. to the present day, and its current Constitution contains explicit provisions on 'the duty of the State to protect and promote the Buddha Sasana' (art. 9). The reciprocal influences, interferences and interactions between monastic and secular laws and

[42] T Bikkhu, *The Buddhist Monastic Code Vol 1: The Patimokkha Training* (Metta Forest Monastery 2007); T Bikkhu, *The Buddhist Monastic Code Vol 2: The Khandhaka Training* (Metta Forest Monastery 2007).
[43] TW Rhys Davids, 'The Pātimokkha', *Sacred Books of the East Vol 13* (Motilal Banarsidass 1996).
[44] M Wijayaratna, *Buddhist Monastic Life: According to the Texts of the Theravāda Tradition* (Cambridge University Press 1990) 143–144.
[45] T Bikkhu (n 42) 12–26.
[46] P Kieffer-Pülz, 'What the Vinayas Can Tell Us About Law' in R Redwood French and MA Nathan (eds), *Buddhism and Law: An Introduction* (Cambridge University Press 2014) 46–62.
[47] J Silk, *Managing Monks: Administrators and Administrative Roles in Indian Buddhist Monasticism* (Oxford University Press 2008); See B Jansen, *The Monastery Rules: Buddhist Monastic Organization in Pre-Modern Tibet* (Paperback, University of California Press 2018).
[48] See M Álvarez Ortega, 'Buddhism and Law' in R. Payne (ed.), *Oxford Bibliographies* (Oxford University Press 2016).
[49] U Singh, 'Governing the State and the Self: Political Philosophy and Practice in the Edicts of Aśoka' (2012) 28 South Asian Studies 131, 131–145.

institutions in Sri Lanka are explored in a series of publications covering the pre-colonial, colonial and post-colonial periods.[50]

In the case of Southeast Asia, since pioneer R. Lingat,[51] there exists a tendency to focus on Burma followed by the key figure of Andrew Huxley. According to the late SOAS scholar, one could speak of a 'Pāli Buddhist law', starting from the idea that the progressive Indianization of South Asia entailed a gradual development of a particular legal praxis and textual tradition (*Dhammathats*), based on the Vinaya literature and Buddhist ethics, from the 13th century until European colonisation.[52] Compared to Burma, the other countries in the area have generated fewer monographic approaches, with Thailand being the primary object of interest.[53]

Finally, in the Himalayan context, in addition to its religious centrality and strong monastic presence, it is widely assumed that Buddhism has played a central role in the Tibetan public sphere since imperial times (7th century), at least at the level of political legitimisation.[54] However, the extent to which the dharma exerted a detectable influence on drafting legal documents or legal praxis remains highly controversial. One of the leading experts on Tibetan law, D. Schuh, has argued that the alleged influence of Buddhism on Tibetan jurisprudence would only be a fictitious construct to guarantee political support;[55] the opposite view to that advocated by Rebecca French, who argues for an omnipresence of Buddhism in Tibetan law, which she refers to in 'cosmological' terms.[56] The unique case of Bhutan, a traditional Buddhist kingdom recently reformed into a modern state, has allowed for interesting reflections in both legal and constitutional terms, such as those of R. Whitecross or local scholar Sonam Kinga1,[57] with articles 2.2. and 3.3. of the Constitution, respectively stating that 'The Chhoe-sid-nyi [dharma and politics] of Bhutan shall be unified in the person of the Druk Gyalpo [King] who, as a Buddhist, shall be the upholder of the Chhoe-sid' and that 'Buddhism is the spiritual heritage of Bhutan, which promotes the principles and values of peace, non-violence, compassion and tolerance.'

[50] B Schonthal, *Buddhism, Politics and the Limits of Law: The Pyrrhic Constitutionalism of Sri Lanka* (First paperback edition, Cambridge University Press 2018).
[51] R Lingat, 'Vinaya et Droit Laïque: Etudes Sur Les Conflits de La Loi Religieuse et de La Loi Laïque Dans l'Indochine Hinayaniste' (1937) 37 Bulletin de l'Ecole Française d'Extrême-Orient 415.
[52] A Huxley, 'Is Burmese Law Buddhist? Transition and Tradition' (2014) 59 Law, Society and Transition in Myanmar, Oxford: Hart Publishing 75.
[53] FE Reynolds, 'Dhamma in Dispute: The Interactions of Religion and Law in Thailand' (1994) 28 Law & Society Review 433, 433–451.
[54] F Pirie, 'Buddhist Law in Early Tibet: The Emergence of an Ideology' (2017) 3 Journal of Law and Religion 406.
[55] D Schuh, 'Recht Und Gesetz in Tibet (Law in Tibet)' in L. Liegt (ed.), *Tibetan and Buddhist Studies Commemorating the 200th Anniversary of the Birth of Alexander Csöma de Körös* (Akadémiai Kiadó 1984).
[56] RR French, *The Golden Yoke: The Legal Cosmology of Buddhist Tibet* (Snow Lion 2002).
[57] R Whitecross, 'Separating Religions and Politics? Buddhism and the Bhutanese Constitution' (Oxford University Press 2013).

4. Animals and Nature in Buddhist Normative Sources.

A specific treatment of animals and nature may observed in the described normative spheres as a concrete projection of their internal logic and varying according to the tradition and context.

Starting with the most general frame, Buddhist Ethics expert Peter Harvey has pointed out that traditional sources do not show a tendency to focus on the opposition of man versus nature but rather stress the contrast between human beings and other sentient beings in terms of agency and spiritual capability. In contrast to modern Western approaches epitomised by the Enlightenment's belief in the conquest of wild nature by man's rationality as a means of development, Buddhist sources would concentrate on the 'privileged' position of being born human. While human beings share with other sentient beings (animals, gods, demi-gods, hell-beings, and hungry ghosts) the experience of suffering and the agency to work towards its removal, they are considered the best possible birth. On the one hand, godly and demonic beings are more harshly stricken by either attachment or aversion. On the other hand, although a noticeably varying degree exists within species, animals have a more limited understanding and capacity for agency (ignorance is their poison), which makes them less suitable for ethical and spiritual development than humans. This superiority would not entail an objectifying commodification of animals, which remain capable of sentiency and suffering. Neither does it imply that nature is a blank scenario for human action. Human agency definitely has karmic consequences on the environment, with which it is embedded in the pervasive notion of interdependence. Between man and nature, there is a strong relationship and dependence, the quality of the moral attitude of people, both by itself (we saw that crops are plentiful in the kingdom of a moral king) and in its treatment of the environment, impacting the flourishing or decline of the habitat as ethical rewards and punishments. There is, thus, a need for harmonious cooperation.[58]

Within general secular ethics, the most commonly alluded reference to the treatment of animals may be found in the first precept, which in Pāḷi reads as follows: *Panatipata veramani sikkhapadam samadiyami (I undertake the precept to refrain from destroying living creatures).* Beyond the apparent intention to prohibit homicide, alike the core precepts of any major religion, the implications of the precept regarding animals vary according to the tradition and context, with 'right livelihood' in the eight-fold noble path excluding trade in living beings and meat.[59] Even when hunting and butchering are considered ignoble and typically low-class or outcast professions, meat consumption is not automatically and universally proscribed, and neither is vegetarianism automatically nor universally required.[60] Within Theravada Buddhism,

there is no general prohibition on eating animals unless they are locally regarded as noble, sacred or particularly unhygienic or dangerous.[61] But it is

[58] Harvey (n 27) 150-153.
[59] Rahula (n 13) 53.
[60] EW Hopkins, 'The Buddhistic Rule against Eating Meat' (1906) 27 Journal of the American Oriental Society 455, 464.
[61] S Mahanarongchai, R Marranca, 'Buddhism, Diet and Vegetarianism' (2007) 12 Thammasat review 1, 2, 3.

considered better to consume 'low' animals (those with lower agency, like fish) while it is controverted if buying meat is immoral or not for encouraging animal killing.[62] In the case of Mahāyāna Buddhism, sources show a more vigorous encouragement for vegetarianism, dwelling on arguments like the previous lives of animals (they were your mother in countless lives) or the pernicious effects on meditative practice and general health.[63] Finally, the Vajrayāna context presents the peculiarity of meat being used in certain tantric rituals, while the harsh regions where it prevails, like the Himalayas, have typically made vegetable scarcity an argument for focusing on compassionate slaughtering rather than strict meat avoidance.[64]

The regulatory constrictions seem to be higher in the case of monastic practitioners, as opposed to regular lay people, drawing both from Vinaya literature and socio-cultural expectations. Monastic Codes clearly prohibit taking the life of animals, either intentionally or unintentionally (even by unwarily dropping water on the ground); but then again, the Buddha explicitly refused to make vegetarianism mandatory for monks.[65] The reasons provided relate to trying to avoid possible monastic schisms based on the issue, considering that rejecting meat food from donors is unwholesome (since it prevents them from acquiring good karma for almsgiving) unless the monks are aware that animals were slaughtered with the very purpose of offering their flesh to them, and, interestingly, discouraging vegetarians from developing self-pride and sense of superiority based on their attachment to virtues and vows.[66] Mahāyāna sources are more prone to encourage vegetarianism for monks, while it is a robust social opinion that monasteries are places of renunciation, which would include meat avoidance. This would explain why East-Asian monasteries are practically all vegetarians.[67]

Finally, regarding the treatment of animals within kingship discourses and historical legal implementations, dharma-abiding monarchs are expected to show concern for animal suffering as an expression of the royal virtue of nonviolence (*ahiṃsā*) and the royal duty to cater for humans, animals, spirits, etc., and their natural habitat highlighted in specific texts.[68] At the same,

---

[62] P Harvey, *An Introduction to Buddhist Ethics. Foundations, Values and Issues* (Cambridge University Press 2000) 162.

[63] DS Ruegg, 'Ahimsa and Vegetarianism in the History of Buddhism' in S. Balasooriya (ed.), *Buddhist Studies in Honour of Walpola Rahula* (George Fraser 1980); TS Shabkar, *Food of Bodhisattvas: Buddhist Teachings on Abstaining from Meat* (Shechen Publications 2008).

[64] G Barstow, *Food of Sinful Demons: Meat, Vegetarianism, and the Limits of Buddhism in Tibet* (Columbia University Press 2017) 90 ff.

[65] A Jagaro, 'Buddhism and Vegetarianism' [1994] True Freedom <http://thaihealingalliance.com/wp-content/uploads/Buddhism_and_Vegetarianism.pdf> accessed 9 September 2024.

[66] Mahanarongchai and Marranca (n 61) 3; JJ Stewart, 'The Question of Vegetarianism and Diet in Pāli Buddhism' (2010) 17 Journal of Buddhist Ethics 99, 101; Harvey (n 27) 160.

[67] J Kieschnick, 'Buddhist Vegetarianism in China' in Roel Sterckx (ed), *Of Tripod and Palate* (Palgrave Macmillan US 2005); AA Tseng, 'Five Influential Factors for Chinese Buddhists' Vegetarianism' (2018) 22 Worldviews: Global Religions, Culture, and Ecology 143; NDB Hiep, S Mahathanadull, 'The Concept and Practices of Mahayana Buddhist Vegetarianism in Vietnamese Society' (2019) 12 The Journal of International Association of Buddhist Universities (JIABU) 77; RM Jaffe, '11. The Debate over Meat Eating in Japanese Buddhism' in W.M. Bodiford (ed.), *Going Forth* (University of Hawaii Press 2017).

[68] For example, the *Cakkavattisīhanāda Sutta* answers to the king that to follow the model of the universal monarch he must: 'govern by Dhamma, and arrange rightful (*dhammika*) shelter, protection and defense for your family, for the army, for your noble warrior client(-king)s, for Brahmin householders, for town-dwellers and countryfolk, for ascetics and Brahmin(-renouncer)s, for animals and birds.' Collins (n 36) 604. A later Mahāyāna discourse, *The Range of the Bodhisattva*, states: 'Your Majesty, a ruler should protect sentient

Emperor Aśoka, considered either an inspiration for or an example of the ideal Buddhist sovereign, incorporated specific provisions addressing these matters in his Pillar and Rock Edicts. Namely, he included animals alongside humans as part of his constituency; he attempted to curb animal suffering by establishing limitations on animal sacrifices and slaughtering days, hunting, and the use of meat in the royal kitchen; and prohibited the gratuitous harm of animals and their habitat. Along with such restrictive measures, the Edicts also contain positive provisions on animal protection, such as medical treatments or setting wells and trees by the roads, allegedly showing a general concern for environmental welfare.[69]

Although scholars like Ian Harris have raised doubts about the 'specifically Buddhist' character of such model references, since Hindu treatises like the *Arthasastra* would show an analogous concern for the welfare of animals,[70] the truth is that countries embracing Buddhism historically show more and clearer instances of legislative implementation. For example, pre-colonial Sri Lankan kings established different restrictions on and prohibitions of animal slaughtering,[71] and even in the complex Vajrayāna context of Tibet, there were legal practices such as the decrees for 'the Protection of Animals and the Environment', issued annually by the 5th Dalai Lama, forbidding 'the killing of all creatures, polluting water sources, depletion of forests, and consequent misuse of the land.[72]'

5. Animals and Environmentalism in Contemporary Buddhist Scholarship.

Besides this classical or historical configuration, Buddhism, a living and dynamic thought system, presents a complex contemporary scenario involving both traditional teachers or scholars (mainly of monastic character) and academic specialists with modern Western-style education.

In traditional contexts, environmentalism is not necessarily a matter of specific study, scholarly interest, or practical concern, as the situation is highly casuistic. Factors such as the urban or remote location of monasteries, the character and relevance of national and local policies, the needs of the community, and the personality and interests of monastic heads create a wide

beings by not burning the habitat or ruining it, etc. A ruler should not vent his anger by burning cities or villages, ruining reservoirs, wrecking dwelling places, cutting down fruit trees, or destroying harvests, etc. In short, it is not right to destroy any well-prepared, well-constructed, and well-extended regions. How is this? These are sources of life used in common by many sentient beings who have not committed any faults. Also, Your Majesty, local deities dwell in these regions, in houses, temples, shrines, groves, etc. If a ruler disrupts these places, then the local deities will be furious. There are also many kinds of animals and other sentient beings existing in these regions that have not committed any faults. If a ruler destroys such regions, these living beings also will be destroyed. Therefore, a righteous ruler should not destroy sentient beings and their habitat. When a ruler does not ruin [the habitat] but protects it, in this way, by protecting it, he also benefits all sentient beings. (…) Your Majesty, a ruler should prepare suitable oblations and offer them [to these spirits]. In this way, then, a righteous ruler protects all sentient beings, chastises the wicked, creates no vice, and, because of this, greatly increases the merit of his own future life. Jamspal and Hackett (n 41) 56-57.

[69] Singh (n 49) 138–140.

[70] I Harris, 'Buddhism and Ecology' in Keown, Damien (ed), *Contemporary Buddhist Ethics* (Curzon 2000) 120.

[71] ARB Amerasinghe, *The Legal Heritage of Sri Lanka* (Royal Asiatic Society of Sri Lanka 1999) 130–133.

[72] L Yangtso, 'Environmentalism in Tibet' (2019) 44 Tibet Journal 39, 40.

spectrum ranging from practically no involvement in environmental initiatives or study to very active participation in programs such as garbage recycling, water sanitation or prevention of animal cruelty and slaughtering, along with targeted scholarship and teaching. Thailand, where the Buddhist sangha plays an important social role, provides plenty of examples of such involvement.[73] I would like, however, to focus on Tibetan Buddhism, drawing from my own in-field and media research.

During the spring and summer of 2013, I conducted a series of semi-structured interviews on Buddhism, Law, Politics, and Social Ethics with fifteen traditional scholars belonging to the four major schools of Tibetan Buddhism in the village of Boudhanath (Kathmandu Valley, Nepal), home to one of the most sacred Vajrayāna Buddhist stupas and more than sixty monasteries. Interestingly, being presented with several contemporary ethical issues, such as gender equality, abortion, or material welfare, environmentalism was the topic that attracted the interest of the fewest informants, while the visit to monasteries would show abundant cases of garbage disposal, water treatment, and general hygiene conditions inconsistent with what we would consider environmental and healthcare awareness.[74] Almost ten years later, the COVID-19 pandemic provided the opportunity to assess the approach and discourses of Tibetan teachers catering for both a local and a global audience through social media. An almost universal feature turned out to be the clear human responsibility in the inception of the epidemic and the external appeal to comply with all the hygienic and sanitary measures established by the authorities, including social distancing, handwashing, masks and vaccinations. The physical (damage of nature), ethical (greed or other immoral behaviour), or esoteric (rage of spirits) character of such human causation was the object of varying singular stress depending on the teacher and audience, with a tendency to represent them as non-exclusive. This points to manifold narrative devices depicting human agency and its impact on animals and their habitat. Consequently, the cultivation of a peaceful mind, the practice of offerings, praying, and rituals were recommended and stressed depending on the audience, along with following the official guidelines, with the latter impacting

[73] For monastic involvement in environmental projects, see VA Sakya, 'Spiritual Connections to Nature and to Climate Change Action' (2023) 111 The Journal of the Siam Society 233, 242–243,where it is stated the monastery of Wat Chak Daeng in Bangkok is considered a community learning center on waste management engaged in study and development of waste recycling processes for all types of waste, and in training on garbage segregation via community leaders to promote waste management behavior at the household level, and to raise awareness and participation among community dwellers regarding environmental issues and waste management.' ; TR Jackson, 'Deep Ecology in Action: A Cross-Cultural Series of Case Studies on the Conservation Efforts of Monks and Religious Leaders in India, Mongolia, and Thailand' (PhD Thesis, University of Pittsburgh 2009) 40-49; RE Talcoth, 'Buddhist Monks and Environmental Issues in Thailand' (PhD Thesis, Chulalongkorn University 2010); for academic debates with traditional Theravada teachers see D Mitchell, W Skudlarek, *Green Monasticism* (Lantern Books 2010).

[74] 'Both a Sakya and a Nyingma scholar referred to a notion of the dual environment (*khor yug*) as outer (nature) and inner (body and mind) entities that need to be purified and protected to grant a profitable human life, whereas a Gelug Rinpoche pointed out that the preoccupation with nature as a support for human existence was already present in vinaya regulations, such as in the precepts dealing with water pollution.' M Álvarez Ortega, 'Traditional Tibetan Buddhist Scholars on Dharma, Law, Politics, and Social Ethics: Philosophical Discussions in Boudhanath (Nepal)' (2018) 4 Buddhism, Law, and Society 1, 23–24.

monastic management in terms of hygiene, waste treatment, and prophylaxis.[75]

The pandemic was also an occasion for the further visibilisation of Tibetan lamas with an already global reach, the most popular of whom is arguably the Dalai Lama. His Holiness drew attention to the pandemic taking place in an already challenging scenario prompted by extreme climate change and wars, reminded about the Buddhist understanding of the world in terms of interdependence and appealed to a 'universal responsibility' which, beyond prayer, required truly global efforts alongside doctors and science.[76] The Dalai Lama devised this responsibility principle as a counterpart to the notion of human rights, among which he undoubtedly includes a 'clean environment' for both present and future generations[77]. He has also shown concern for animal suffering and promoted vegetarianism, though he is not a vegetarian himself, as advised by his doctor.[78]

These last issues have been the focus of interest of Khenpo Tsultrim Lödro, a reputable teacher from Larung Gar, probably the most extensive religious setting in Tibet. In a series of writings and speeches and as part of a larger project of moral regeneration, Tsultrim Lödro has tackled the conditions of animals among nomads on the Tibetan plateau, pleading for a stop from selling livestock to slaughterhouses in exchange for fast cash (sometimes used to buy guns and generate further violence), advocating for more compassionate methods of slaughter, and asking lay people to eat less meat and not use fur clothing.[79] In the case of monastics, giving up meat, even if not imposed, is strongly recommended:

'Vegetarianism is the cause of a healthy body as well as peace in one's surroundings. It is also food in harmony with the path to liberation and bodhicitta. Consuming meat is the means to defeating in a single stroke: the welfare of animals, one's own health, and one's path to liberation in future lives. Friends, I urge you to keep love and compassion in your mind. I invite you to join the ranks of those who live as vegetarians.[80]'

These traditional teachers constitute a minority. The bulk of the scholarly literature on Buddhist environmentalism has been developed by University academics, so much so that it has been argued that contemporary interest responds mainly to a Western influence.[81] The question of whether Buddhism is traditionally and intrinsically ecology-oriented is a complex issue that raises

[75] See extensively M Álvarez Ortega, 'Global Virus, International Lamas: Tibetan Religious Leaders in the Face of the Covid-19 Crisis' in Kaesehage, Nina (ed), *Religious Fundamentalism in the Age of Pandemic* (Transcript 2021).
[76] ibid 190–193.
[77] The 14th Dalai Lama, 'A Clean Environment Is a Human Right' (*The 14th Dalai Lama*, 10 September 2024) <https://www.dalailama.com/messages/environment/clean-environment> accessed 11 September 2024.
[78] 'Nine Questions About Vegetarianism' (*FPMT*) <https://fpmt.org/mandala/archives/mandala-issues-for-2011/january/nine-questions-about-vegetarianism/> accessed 11 September 2024.
[79] See H Gayley, 'The Compassionate Treatment of Animals: A Contemporary Buddhist Approach in Eastern Tibet' (2017) 45 Journal of Religious Ethics 29.
[80] ibid 41.
[81] See in detail I Harris, 'How Environmentalist Is Buddhism?' (1991) 21 Religion 101; I Harris, 'Buddhist Environmental Ethics and Detraditionalization: The Case of ecoBuddhism' (1995) 25 Religion 199.

questions of anachronism (environmentalism is globally a recent phenomenon) and the limits between merely describing a tradition or developing and proposing ethical stances based upon or in harmony with such a tradition, something which is not always clearly stated or justified by authors. In any case, most scholars share a similar take in grounding their ecological discourses upon core Buddhist notions. Thus, the understanding of the world as an interdependent reality (*pratityasamutpada*) and karma as a result of agency typically lead to emphasising that all beings and phenomena are interconnected, implying that human actions affect the entire ecosystem and hence identifying an ethical responsibility that resonates with environmentalism. At the same time, the concepts of compassion and no-violence would be extended to the environment, encouraging the protection of ecosystems and avoidance of actions that cause harm to animals and nature. Finally, the ideas of simplicity and non-attachment would encourage a Buddhist ideal of living simply and being content with fewer material goods, which aligns with sustainable living practices.[82]

The discussion of animal rights, on the other hand, would constitute a more convoluted theoretical scenario since the very notion of (human) rights receives varied treatment within Buddhist scholarship. Ethical debates at the turn of the century showed that while some academics find the concept of human rights to be a valuable legal and political instrument to protect from suffering and allow development (including dharma) justified by the unique human capacity and agency,[83] others reject it altogether as a construct which contradicts emptiness and promotes entitlement, attachment, and greed.[84] A third group considers the notion unreasonably restricted for humans and rather advocates for an extension to all sentient beings with which humans share the experience of suffering.[85] It is with the logic of this last group that recent academic works developed their specific defense of 'animal rights' as a reasonable consequence of Buddhist ethics in dialogue with well-known Western proposals such that of Peter Singer.[86]

At the sociopolitical level, it is important to note that these ideas did not just remain in the theoretical realm, inspiring activism and several organised movements generically referred to as 'Eco-Buddhism,' such as the International

[82] ME Tucker, DR William (n 31); De Silva (n 31); Sahni (n 31); James (n 31); LE Sponsel, P Natadecha-Sponsel, 'Buddhist Environmentalism' [2016] Teaching Buddhism: New Insights on Understanding and Presenting the Traditions 318.

[83] S Promta, 'A Concept of Rights in Buddhism' (2002) 1 The Chulalongkorn Journal of Buddhist Studies 17, 26; P Schmidt-leukel, 'Buddhism and the Idea of Human Rights: Resonances and Dissonances'' (2006) 26 Buddhist-Christian Studies 33, 52.

[84] CK Ihara, 'Why There Are No Rights in Buddhism: A Reply to Damien Keown', *Buddhism and human rights* (Routledge 2012) 48; S Arguilère, 'Peut-on Parler Des Droits de l'Homme Dans Le Bouddhisme?', *Le Bouddhisme et ses Normes: Traditions-Modernités* (Presses Universitaires de Strasbourg 2006) 148 ff.

[85] PD Junger, 'Why the Buddha Has No Rights', *Buddhism and Human Rights* (Routledge 2012) 62–63; JU Sobisch, T Brox, 'Translations of Human Rights. Tibetan Contexts' in C. Meinert and H. Zöllner (eds), *Buddhist Approaches to Humans Rights: Dissonances and Resonances* (Transcript 2010) 176; MT Adam, 'Buddhism, Equality, Rights' (2013) 20 Journal of Buddhist Ethics 422, 421–443.

[86] See N Phelps, *The Great Compassion: Buddhism and Animal Rights* (Lantern Books 2004); P Waldau, 'Buddhism and Animal Rights' in D. Keown (ed.), *Contemporary Buddhist Ethics* (Routledge 2013).

Network of Engaged Buddhists (INEB), Green Buddhism, The Buddhist Climate Action Network, or Dharma Voices for Animals.[87]

6. An Implementation Case: The Kingdom of Bhutan.

A lingering question remains about the actual legislative incorporation and effective implementation of the values, models, and goals contained in the normative models. It does thus seem appropriate to look at, even if very briefly, a case of a country typically presented as a living example: the Himalayan landlocked Kingdom of Bhutan.

Founded in the 17th century by monastic elites fleeing Tibet, Bhutan is considered to have functioned as a Buddhist Vajrayāna theocracy until the beginning of the 20th century when it became a monarchy. In 2008, the country experienced a process of constitutionalization promoted by the king, establishing, as mentioned above, a Dual System of Government (*Chhoe-sid-nyi* [dharma and politics]) and Buddhism as the 'spiritual heritage' of the country, promoting peace, non-violence, compassion, and tolerance.

Bhutan has established strong environmentalist legislation, policies and goals. At the constitutional level, there is a mandate to maintain at least 60% forest cover for all time (art. 5.3), which, along with a battery of measures, has made Bhutan the first and one of the few carbon-negative countries in the world.[88] The choice for 'high value, low volume' tourism means that only relatively few high-profile tourists, who pay environmental taxes, visit the country annually. Hunting activities are largely prohibited, especially in reserved forests and protected areas, with limited exceptions, such as subsistence hunting by Indigenous communities in remote regions,[89] and slaughterhouses are heavily regulated, with meat commerce being forbidden on Buddhist auspicious dates and the first month and fourth months of the Bhutanese calendar.[90] At the same time, issues of religious freedom have been raised by minorities who continue practising animal sacrifices, even if discreetly.[91]

Despite the expected tensions with local practices and economic considerations that might challenge viability in the future,[92] and though there is room for speculation on the varied motivations for this ecological agenda—including strategies of international marketing or protection of local spirits — it seems a fair assessment to consider Bhutan as an exemplary case of national

[87] Each of these organisations possess their own website containing their principles an goals. An overview may be found at S Kaza, 'To Save All Beings: Buddhist Environmental Activism' in R. S. Gottlieb (ed.), *This Sacred Earth. Religion, Nature, Environment* (Routledge 2003) 304-311.
[88] D Yangka, V Rauland and P Newman, 'Carbon Neutral Policy in Action: The Case of Bhutan' (2019) 19 Climate Policy 672.
[89] See mainly the Forest and Nature Conservation Act of Bhutan, 1995.
[90] See mainly Livestock Act of Bhutan, 2001
[91] D Lee, 'Here There Be Dragons! Buddhist Constitutionalism in the Hidden Land of Bhutan' (2014) 15 Australian Journal of Asian Law 17, 28 ff.
[92] See M Miyamoto, J Magnusson and FJ Korom, 'Animal Slaughter and Religious Nationalism in Bhutan' (2021) 80 Asian ethnology 121; B Ghosh, S Chakraborty, 'Implications of Paradigm Shift in Tourism Policy: An Evidence of Bhutan' (2020) 13 Prabandhan: Indian Journal of Management; U Tshewang, MC Toabias and JG Morrison, *Bhutan: Conservation and Environmental Protection in the Himalayas* (Springer 2021).

prioritising of animal protection and environmentalism explicitly based upon universalising Buddhist values.[93]

7. Concluding remarks.

This paper has attempted to present an overview of Buddhist normative responses regarding animals, nature, and environmentalism. In contrast to simplifying and essentialising idealisations, the overall picture is a complex and rich tapestry prompted by diversity, internal and external tensions, and potentialities.

Buddhist ethics is highly gradualistic, contextual, and casuistic rather than hard-core deontological, meaning that the ideal goal of not inflicting suffering on any living creature is in tension with a plural reality of socio-cultural dynamics and contexts, resulting in exigencies of different intensity depending on the agent (e.g., rulers, monastics, laypeople) and their situation, and the resort to exceptions (donor offerings) and loopholes (slaughtering outsourced to low casts or imported). In any case, traditional sources do not condone a general imposition of vegetarianism.

This leads to another tension between local and Western approaches and priorities, exemplified by the opposition between modern and traditional scholars. The latter are generally less prone to develop a specific interest and exigent discourses on environmentalism and vegetarianism, with more local sensibility and an advisory tone, and usually an external exposure. Western academics, on the other hand, have made Buddhist environmentalism a research field dedicated to exploring the potentialities of Buddhist concepts and understanding to create a theoretical corpus to address animal issues and ecology in a comprehensive fashion. The debate on animal rights is an excellent example of the diversity of stances and the Western influence of these proposals.

Finally, the Buddhist Kingdom of Bhutan, one of the most environmentally committed countries in the world, provides a practical and concrete implementation scenario for the aforementioned tensions, complexities, and potentialities.

[93] See, e.g., S Lhundup, 'The Genesis of Environmental Ethics and Sustaining Its Heritage in the Kingdom of Bhutan 2002 Student Notes Issue: Graduate Note' (2001) 14 Georgetown International Environmental Law Review 693.

Gaeta MC, 'Intelligenza artificiale sostenibile e tutela dei green rights' (2024) 2 EJPLT, 147 – 171.
DOI: https://doi.org/10.57230/EJPLT242MCG

EJPLT
ISSN 2704-8012



Intelligenza artificiale sostenibile e tutela dei *green rights*

Sustainable artificial intelligence and the protection of green rights

MARIA CRISTINA GAETA
Appointed Lecturer in Green Law and Green Mobility
Module Leader Jean Monnet Chair EUGREENEXT
Università degli Studi Suor Orsola Benincasa
Senior Researcher ReCEPL

Abstract

Lo scenario contemporaneo caratterizzato dalla rapida diffusione ed evoluzione dell'Intelligenza Artificiale (IA) impone necessarie riflessioni sulla sostenibilità della stessa nella prospettiva antropocentrica della tutela dell'essere umano. Ciò implica, in primo luogo, di indagare la tutela di quei diritti dell'uomo che vengono reinterpretati nella prospettiva della sostenibilità ambientale (green rights), poi approfondita anche nelle altre sue declinazioni. Allo stesso tempo, però, risulta di fondamentale importanza stabilire il perimetro dell'operatività dell'IA al fine di limitarne i rischi per l'essere umano e per i propri diritti, anche tramite adeguati strumenti di diritto privato per la sostenibilità: dalla responsabilità digitale d'impresa, ai contratti d'impresa, con una particolare attenzione alla misurazione dell'impatto dell'IA e considerando, anche, i c.d. fattori ESG.

* L'articolo è co-finanziato dalla Cattedra Jean Monnet "*European Green rights: reshaping fundamental rights for next generations*" (EUGREENEXT) presso l'Università degli Studi Suor Orsola Benincasa (UNISOB), titolare della cattedra Prof.ssa Ilaria A. Caggiano, 2022-2025, bando ERASMUS-JMO-2021-HEI-TCH-RSCH, progetto n. 101047962. www.eugreenext.eu

© The author(s) 2024, 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 contemporary scenario characterised by the rapid diffusion and evolution of Artificial Intelligence (AI) imposes necessary reflections on its sustainability from the anthropocentric perspective of the protection of human beings. This implies, first of all, investigating the protection of those human rights that are reinterpreted in the perspective of environmental sustainability (green rights), which is then deepened in its other declinations. At the same time, however, it is of fundamental importance to establish the perimeter of AI's operation in order to limit its risks for human beings and their rights, also by means of appropriate private law instruments for sustainability: from corporate digital responsibility to business contracts, with a focus on measuring the impact of AI and also considering the so-called ESG factors.

Keywords: sustainable AI; green rights; ESG; diritti per la natura; RDI; misurazione della sostenibilità; contratti verdi; clausole di sostenibilità.

Summary: 1. Intelligenza artificiale e sostenibilità. – 2. Dalla regolamentazione della sostenibilità ambientale ai c.d. fattori ESG. – 3. Diritto privato e tutela preventiva della sostenibilità. – 3.1. La qualificazione giuridica della natura nella dicotomia soggetto-oggetto del diritto. – 3.2. Responsabilità digitale d'impresa e meccanismi di misurazione. – 3.3. Contratti d'impresa a garanzia della sostenibilità dell'intelligenza artificiale. – 4. Sviluppo sostenibile dell'IA nella prospettiva della tutela dei *green rights*.

1. Intelligenza artificiale e sostenibilità.

Le nuove tecnologie non possono essere considerate intrinsecamente positive o negative, ma è l'uso che ne viene fatto a determinarne il loro impatto e ciò vale anche, e soprattutto, per i sistemi di intelligenza artificiale. Appare quindi di fondamentale importanza garantire lo sviluppo di un'IA sostenibile (*Sustainable AI*), intesa sia come IA impiegata in modo etico e responsabile (*Sustainability of AI*), che come IA in grado di perseguire obiettivi di sostenibilità (*AI for Sustainability*) potendo essere essa stessa strumento di sostenibilità o per il perseguimento della sostenibilità[1].

Nel contesto della tutela ambientale e nell'ottica della protezione delle generazioni future, ad esempio, l'IA può essere impiegata per ottimizzare i processi industriali e ridurre gli sprechi energetici, ovvero può risultare un prezioso strumento per l'efficientamento delle risorse e della produzione energetica da fonti rinnovabili. L'IA consente, altresì, di sviluppare sistemi di monitoraggio ambientale più efficaci e accurati grazie ai suoi modelli di analisi

[1] Sviluppare un'IA sostenibile significa sviluppare un'IA che sia compatibile con la tutela delle risorse ambientali per le generazioni attuali e future, nonché con i modelli economici per le società e con i valori sociali fondamentali per una determinata società. L'Intelligenza Artificiale Sostenibile implica oggi, infatti, un funzionamento responsabile delle tecnologie di IA, con particolare attenzione al piano ambientale sociale ed economico. Allo stesso tempo, però sviluppare un'IA sostenibile implica anche, un utilizzo dell'IA come strumento per affrontare direttamente le sfide ambientali sociali ed economiche. Essa mira a garantire la sostenibilità, ponendo rimedi, ad esempio, al cambiamento climatico, prevedendo una migliore gestione delle materie prime, imponendo scelte non discriminatorie sul piano sociale e garantendo una migliore allocazione delle risorse economiche. Cfr. A. VAN WYNSBERGHE, *Sustainable AI: AI for sustainability and the sustainability of AI*, in *AI and Ethics*, 2021, I, 214 - 215, DOI: https://doi.org/10.1007/s43681-021-00043-6.

in grado di tenere conto e combinare un elevatissimo numero di fattori per restituire un'immagine molto più precisa dell'attuale situazione climatica, anche con un indice di predittività piuttosto accurato delle prospettive future sulla base dello stato dell'arte. Ciò permette di ridurre l'impatto ambientale delle attività umane e promuovere pratiche concretamente eco-sostenibili, garantendo un approccio protettivo per quei diritti dell'uomo tutelati dalla Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza)[2] di maggiore rilievo in questo contesto: la dignità umana (art. 1), l'uguaglianza e la non discriminazione (artt. 20 e 21), la salute (art. 35) l'ambiente (art. 37), ma anche la proprietà (art. 17), la tutela dei consumatori (art. 38) e la *privacy* (artt. 7 e 8). Tali diritti fondamentali devono quindi essere reinterpretati per rispondere alle esigenze delle generazioni presenti e future, alla luce del concetto di sostenibilità, sviluppato anche a livello europeo, potendo essere così definiti *green rights*[3].

Risulta di fondamentale importanza stabilire il perimetro dell'operatività dell'intelligenza artificiale onde evitarne (o per certi versi limitarne) un impatto negativo sull'ambiente, ad esempio dovuto al c.d. inquinamento digitale (*digital pollution*)[4], che è strettamente connesso all'impronta ecologica di ciascun individuo (*ecological footprint*)[5]. Il riscaldamento terrestre dovuto al consumo di energia elettrica, anche connesso all'utilizzo delle nuove tecnologie, la difficoltà di smaltimento di alcune fonti energetiche, come le batterie al litio, ovvero le emissioni di CO_2 e altri gas serra per l'utilizzo di determinati prodotti, anche intelligenti, sono solo alcuni degli esempi connessi all'inquinamento ambientale causato dalle tecnologie di IA.

Da non trascurare, poi, è l'impatto che l'IA può avere direttamente sull'essere umano, come nel caso della violazione della libertà personale derivante dal monitoraggio sistematico e su larga scala, o di decisioni automatizzate potenzialmente discriminatorie per il consumatore, che implicano un evidente impatto sulla società.

Infine, da non sottovalutare sono anche i profili di sostenibilità economica dell'IA, che si fondano sulla necessità di assicurare che i benefici economici

---

[2] Carta dei diritti fondamentali dell'Unione europea, 2000/C 364/01 (Carta di Nizza).

[3] Il concetto di "*green rights*" è stato sviluppato nel corso dei tre anni (2022-2025) del progetto della Cattedra Jean Monnet "*European Green rights: reshaping fundamental rights for next generations*" (EUGREENEXT) presso l'Università degli Studi Suor Orsola Benincasa (UNISOB), coordinato dalla Prof.ssa Ilaria A. Caggiano in qualità di *Chair Holder*, bando ERASMUS-JMO-2021-HEI-TCH-RSCH; progetto n. 101047962.

[4] Per inquinamento digitale si intende l'insieme dei danni ambientali causati dall'utilizzo e dal consumo energetico delle tecnologie digitali (es. *smartphone*, *computer*, *server* e infrastrutture di rete) prime tra tutte quelle rientranti nel dominio dell'*Internet of Things* (IoT), che immettono grandi quantità di CO_2 e altri gas serra nell'atmosfera, lasciando un'evidente traccia del livello di inquinamento causato da tecnologie digitali.

[5] Per le aziende l'impronta di carbonio (*Carbon Footprint*) è particolarmente significativa, in quanto prende in considerazione le emissioni dirette e indirette di gas serra per le quali l'azienda è responsabile. La *Carbon Footprint*, è un indicatore ambientale che misura l'impatto delle attività umane sul clima globale, ed esprime in modo quantitativo gli effetti delle emissioni di gas serra prodotti da un'organizzazione, un prodotto o un servizio. In tal senso H. FERREBOEUF et al., *Lean ICT - towards digital sobriety*, report del *working group* del *think tank* di "*The shift project*", marzo 2019, 17, disponibile al link https://theshiftproject.org/wp-content/uploads/2019/03/Lean-ICT-Report_The-Shift-Project_2019.pdf,v hanno stimato il 4% di emissioni prodotte dalle tecnologie digitale, mentre nello studio di C. FREITAG, M. BERNERS-LEE, K. WIDDICK et al., *The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations,* in *Patterns*, Vol. 2, IX, 1-2, disponibile al link: https://www.sciencedirect.com/science/article/pii/S2666389921001884 sono stati stimati valori compresi tra l'1,8 e il 2,8% di emissioni prodotte dal digitale. Nonostante la discordanza dei valori, in entrambi gli studi viene messo in evidenza il fenomeno dell'inquinamento digitale e come questo sia destinato ad aumentare.

siano distribuiti in modo equo tra tutte le persone e le comunità a livello mondiale, rispetto alle esigenze attuali, ma senza compromettere la capacità delle future generazioni di soddisfare le proprie. Ciò richiede un ponderato e bilanciato investimento economico, che tenga conto della crescita economica a lungo termine e dell'uso efficiente delle risorse per massimizzare i benefici economici. Ecco che il concetto di sostenibilità diventa essenziale non solo per la tutela dell'ambiente, ma anche direttamente per la tutela della società (sostenibilità sociale) e dell'economia (sostenibilità economica).

Pertanto, l'IA va opportunamente regolamentata per garantire un'innovazione sostenibile e in questa direzione muove anche l'AI Act[6], seppure con le sue criticità applicative. Promuovere pratiche responsabili – dalla progettazione e implementazione, alla gestione dei sistemi basati su IA sia come prodotto dell'attività aziendale che come strumento per lo sviluppo della stessa – è essenziale per garantire la protezione delle generazioni future anche rispetto allo sviluppo tecnologico, ponendo proprio le tecnologie di IA al servizio dell'uomo e del proprio benessere.

2. Dalla regolamentazione della sostenibilità ambientale ai c.d. fattori ESG.

Il concetto di sviluppo sostenibile sembra risalire al 1987 quando la Commissione mondiale sull'ambiente e lo sviluppo (WCED) utilizzò il termine nel Rapporto Brundtland, intitolato *«Our Common Future»*[7]. Secondo la Commissione, per «sostenibilità» deve intendersi il soddisfacimento delle esigenze delle generazioni presenti senza danneggiare quelle delle generazioni del domani. Tale concetto ruota attorno a due punti fondamentali: l'equità intra-generazionale, ovvero la necessità di soddisfare le esigenze del mondo povero, migliorandone le condizioni, e l'equità inter-generazionale, che si traduce nell'opportunità di limitarsi nello sfruttamento dell'ambiente per evitare di danneggiare le generazioni future.

Così definito lo sviluppo sostenibile trova una sua prima applicazione in relazione alla sostenibilità ambientale e, nello specifico, all'importanza di tutelare l'ambiente affinché ne possano godere anche le generazioni future. Tale principio è stato esplicitato anche nella Dichiarazione sulle responsabilità delle generazioni presenti verso le generazioni future dell'UNESCO, firmata a Parigi dieci anni dopo (12 novembre 1997)[8]. La Dichiarazione dell'UNESCO sottolinea, infatti, la responsabilità delle generazioni presenti di trasmettere a quelle future una Terra non irrimediabilmente danneggiata a causa dell'attività umana, usufruendo delle risorse naturali in maniera ragionevole (art. 4). Allo stesso tempo, nella Dichiarazione si invitano le generazioni presenti ad impegnarsi per uno «sviluppo durevole» e a preservare le condizioni di vita e in

[6] Regolamento del Parlamento europeo e del Consiglio, Reg. 2024/1689/UE del 13.06.2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica Reg. n 300/2008/UE, n. 167/2013/UE, n. 168/2013/UE, n. 2018/858/UE, n. 2018/1139/UE e n. 2019/2144/UE, e le Direttive n. 2014/90/UE, n. 2016/797/UE e n. 2020/1828/UE (Regolamento sull'intelligenza artificiale – *Artificial Intelligence Act*, in sigla AIA).

[7] Report of the World Commission on Environment and Development (WCED), *Our Common Future*, 1987.

[8] Organizzazione delle Nazioni Unite per l'Educazione, la Scienza e la Cultura (UNESCO), *Dichiarazione sulle responsabilità delle generazioni presenti verso le generazioni future*, Parigi, 12 novembre 1997.

particolare la qualità e l'integrità dell'ambiente, affinché le generazioni future non siano esposte a eccessivi inquinamenti e, in generale, a danni ambientali tali da mettere in pericolo la loro salute o addirittura la loro vita (art. 5). La Dichiarazione, in particolare, invita a preservare per le prossime generazioni le risorse naturali necessarie al mantenimento della vita e al suo sviluppo, nonché a prendere in considerazione le possibili conseguenze delle proprie azioni per le generazioni future (art. 5).

In questa definizione di sostenibilità spicca in primo piano per le istituzioni internazionali ed europee quella dell'eco-sostenibilità, connotata per l'appunto nella prospettiva della tutela ambientale. Essa è ormai disciplinata da una regolamentazione "verde" multilivello (europea e internazionale, in primo luogo, e poi nazionale), composta da diverse tipologie di atti normativi: non solo di *hard law* (atti normativi vincolanti) ma anche di *soft law* (dalle linee guida ai codici di condotta)[9], oltre che da precise norme tecniche (in particolare gli standard).

In tale prospettiva le *Conferenze delle Parti* (c.d. COP) ratificanti la Convenzione Quadro delle Nazioni Unite sui Cambiamenti Climatici[10], hanno assunto un ruolo crescente all'interno del dibattito internazionale sul contrasto ai cambiamenti climatici, a partire dall'adozione, nel 2015, di un accordo universale e giuridicamente vincolante sul clima durante la COP21 (Accordo di Parigi) [11], poi rinnovato con il "Patto per il clima", durante la COP26 di Glasgow nel 2021[12], recentemente messi in discussione negli Stati Uniti d'America[13].

D'altra parte, anche l'Unione europea è da sempre attiva in tutti gli ambiti della politica ambientale e di sviluppo sostenibile, fondando la propria strategia sui principi della precauzione, dell'azione preventiva e della

[9] Per quanto riguarda la disciplina delle nuove tecnologie in un'ottica di sostenibilità ambientale, un'efficace disciplina di diritto privato dovrebbe tener conto anche dei principi etici, eventualmente contenuti anche in norme *soft law* con un importante ruolo di orientamento degli *stakeholder*, anche se non da soli sufficienti per una completa regolamentazione di un fenomeno che necessita di regole vincolanti. Cfr.: M.L. GAMBINI, *Algoritmi e sicurezza*, in *Giur. It.*, 2019, 7, 1657, che sottolinea che la *soft law* non appare sufficiente, poiché la sua efficacia dipende dall'adeguamento spontaneo degli operatori. Per una panoramica sull'efficacia delle norme di *soft law* e sulla loro collocazione nelle fonti del diritto cfr. A. IANNOTTI DELLA VALLE, *Le regole di Internet tra poteri pubblici e privati. Tutela dei diritti e ruolo dell'antitrust in una prospettiva costituzionale*, ES, Napoli, 2023, 42 ss.; A. IANNOTTI DELLA VALLE, *L'età digitale come "età dei diritti": un'utopia ancora possibile?, Federalismi.it*, 2019, XVI, 10; A. IANNOTTI DELLA VALLE, *La giurisdizione privata nel mondo digitale al tempo della crisi della sovranità: il "modello" dell'Oversight Board di Facebook*, *Federalismi.it*, 2021, XXVI, 144 ss.; E. MOSTACCI, *La soft law nel sistema delle fonti: uno studio comparato,* Padova, 2008; A. SOMMA, *Soft law e hard law nelle società postmoderne,* Torino, 2009. Per approfondire "Il ruolo delle linee guida in materia ambientale" si veda C. INGENITO in *Rivista Giuridica Ambiente Diritto*, 2019, III, 6 ss..

[10] Conferenza sull'Ambiente e sullo Sviluppo delle Nazioni Unite (UNCED), Convenzione quadro delle Nazioni Unite sui cambiamenti climatici (*United Nations Framework Convention on Climate Change* - UNFCCC o FCCC), nota anche come Accordi di Rio, 9.05.1992, entrata in vigore il 21.05.1994.

[11] Conferenza delle Parti della Convenzione quadro delle Nazioni Unite sui cambiamenti climatici (COP21 dell'UNFCCC), Accordo di Parigi del 12.12.2015.

[12] Conferenza delle Parti della Convenzione quadro delle Nazioni Unite sui cambiamenti climatici (COP21 dell'UNFCCC), Patto per il clima di Glasgow (*Glasgow Climate Pact*) del 13.11.2021.

[13] Appare opportuno evidenziare che a partire dalla vittoria delle elezioni del Presidente degli Stati Uniti d'America, nel novembre 2024, Donald Trump stia considerando di far uscire gli USA dall'Accordo di Parigi e che sia già in preparazione l'ordine esecutivo sull'abbandono dell'Accordo. Il neo-rieletto Presidente ha dichiarato di voler promuovere l'espansione dei combustibili fossili e in questo senso pare voler rinunciare alla *leadership* americana in materia di tutela ambientale ponendosi in contrasto anche con i principi del *Green Deal* europeo, D. GELLES, *Trump Whiplash Looms Over Global Climate Talks*, in *The New York Times*, 7.11.2024, accessibile al seguente link: https://www.nytimes.com/2024/11/07/climate/trump-climate-cop-negotiations.html.

correzione alla fonte dei danni causati dall'inquinamento, nonché sul principio «chi inquina paga». La relativa base giuridica è rinvenibile negli articoli 11 e da 191 a 193 del TFUE. Di recente, poi, l'UE ha intrapreso un percorso finalizzato alla riduzione dell'impatto ambientale per raggiungere, entro il 2050, il c.d. *Net Zero*, uno scenario di economia a zero emissioni nette di gas serra, basato su un meccanismo di compensazione che vada a neutralizzare ciascuna emissione prodotta. In questo contesto di iniziativa eurounitaria si colloca nel 2019 il *Green Deal* europeo[14], che mira a raggiungere una proficua coesistenza di sviluppo economico e sociale, nonché la neutralità climatica, attraverso una strategia di investimenti in tecnologie verdi, soluzioni sostenibili e rispettose dell'ambiente, da bilanciare con l'attività d'impresa. Seguendo i principi del *Green Deal* e per la loro applicazione, l'assunzione di debito comune ha consentito di istituire il c.d. *Recovery Plan* dell'Unione europea (*Next Generation EU* – NGEU)[15], che della transizione ecologica fa uno dei suoi pilastri. Il NGEU, come è noto, ha ricevuto attuazione in Italia con il Piano Nazionale di Ripresa e Resilienza (PNRR) del 2021[16], che tra le sue missioni ha quella della rivoluzione verde e della transizione ecologica (Missione 2), nonché quella relativa allo sviluppo delle infrastrutture per la mobilità sostenibile (Missione 3). Il PNRR rappresenta una svolta ed è già una pietra miliare nel cammino della tutela dell'ambiente in un'ottica sostenibile, nella direzione già fissata a livello europeo. Inoltre, l'attuale crisi energetica pone ulteriori sfide, che devono essere affrontate accelerando ulteriormente gli obiettivi di transizione ecologica e, su questo aspetto, assume valenza strategica il piano *RePowerEU* del 2022[17].

Nel contesto di tutela ambientale sopra delineato, la Commissione europea nel luglio 2021 ha adottato il *Fit for 55*, un pacchetto di riforme e regolamenti economici e sociali che costituisce parte integrante del *Green Deal* europeo e che si propone di ridurre, entro il 2030, le emissioni del 55% rispetto ai livelli del 1990, per poi arrivare al *Net Zero* entro il 2050. Sulla riduzione delle emissioni di gas a effetto serra di particolare rilievo è anche la comunicazione europea "*Pronti per il 55 %": realizzare l'obiettivo climatico dell'UE per il 2030 lungo il cammino verso la neutralità climatica*"[18]. La comunicazione contiene un pacchetto di proposte interconnesse e illustra le misure scelte, evidenziando

[14] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, il *Green deal europeo*, 11.12.2019, com(2019) 640. Nella stessa direzione di garantire e implementare la sostenibilità muove il "Nuovo Bauhaus europeo", un'iniziativa europea atta a sviluppare un movimento creativo e interdisciplinare che collega il *Green Deal* europeo alla vita quotidiana dei cittadini dell'UE con il fine di rendere la vita più accessibile (anche economicamente), ripensare un modo di vivere sostenibile, migliorare la qualità dell'esperienza di vita dei cittadini europei e incentivare l'innovazione in tale ambito. Per un approfondimento sul governo della sostenibilità e dei suoi costi, anche con riguardo al "Nuovo Bauhaus europeo", si veda M. Francesca, *Tre appunti in materia di sostenibilità, welfare e Bauhaus europeo,* in *EJPLT,* 2024, II, 5 - 7. Per maggiori dettagli sul "Nuovo Bauhaus europeo" si rinvia alla pagina ufficiale della Commissione europea: https://culture.ec.europa.eu/it/node/1181.

[15] *Next Generation EU* (NGEU), proposto dalla Commissione europea il 27.05.2020 e approvato dal Consiglio nella riunione straordinaria del 21.07.2020, EUCO 10/20.

[16] Piano Nazionale di Ripresa e Resilienza (PNRR), definitivamente approvato in Italia il 13.07.2021, a seguito della decisione di esecuzione del Consiglio dell'Unione europea del 6.07.2021, n. 10160/2.

[17] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Piano *REPowerEU*, 18.5.2022, COM(2022)230 final.

[18] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, "Pronti per il 55 %": realizzare l'obiettivo climatico dell'UE per il 2030 lungo il cammino verso la neutralità climatica, 14.07.2021, COM(2021)550.

come il pacchetto raggiunga l'equilibrio tra equità, riduzione delle emissioni e competitività[19].

Passando poi alla recente normativa di *hard law*, la *European Climate Law* (Regolamento 2021/1119/UE)[20] traduce in norme regolamentari l'obiettivo europeo di raggiungere la neutralità climatica entro il 2050. Si tratta di un nuovo e più ambizioso obiettivo rispetto a quello che era stato inizialmente indicato per il 2030 nel Regolamento 2018/1999/UE[21] e, soprattutto, nel Regolamento 2018/842/UE[22] (riduzione di almeno il 40% delle emissioni nel 2030, rispetto ai valori del 1990)[23].

Nello specifico, il Reg. 2018/1999/UE è stato recepito in Italia nel Piano Nazionale Integrato per l'Energia e il Clima (PNIEC)[24], il quale definisce la politica energetica e climatica del Paese a lungo termine. Esso fornisce una visione strategica per la transizione energetica e l'azione climatica, identificando gli obiettivi, le politiche e le misure necessarie.

Come evidenziato, il concetto di tutela ambientale appare centrale per l'UE la quale con molteplici politiche e regolamentazioni mira a tutelare l'ambiente. Anche il recente Regolamento 2024/1991/UE[25] sul ripristino della natura dimostra la forte attenzione europea per la sostenibilità ambientale.

Anche in Italia, però, la tematica della protezione dell'ambiente è centrale. I principi cardine sulla tutela ambientale sono ora espressamente sanciti dalla Costituzione e già da tempo regolati dal Testo Unico Ambiente (D.Lgs.

---

[19] Detti obiettivi sanciti dal *Fit for 55*, sono stati riconfermati di recente da Ursula von der Leyen, nel suo discorso di reinsediamento per la sua nuova elezione a Presidente della Commissione europea, nell'ambito degli obiettivi del *Green Deal*, annunciando, però, un cambio di approccio: il raggiungimento della neutralità climatica sarà promosso puntando maggiormente su tecnologie innovative come i carburanti sintetici (*E-fuel*) per il raggiungimento dell'obiettivo di riduzione delle emissioni di CO_2 del 100%, entro il 2035.

[20] Regolamento 2021/1119/UE del Parlamento europeo e del Consiglio, 30.06.2021 che istituisce il quadro per il conseguimento della neutralità climatica e che modifica il regolamento (CE) n. 401/2009 e il regolamento (UE) 2018/1999, Normativa europea sul clima (*European Climate Law*).

[21] Regolamento 2018/1999/UE del Parlamento europeo e del Consiglio, 11.12.2018, sulla governance dell'Unione dell'energia e dell'azione per il clima che modifica le direttive 663/2009/CE e 715/2009/CE del Parlamento europeo e del Consiglio, le direttive 94/22/CE, 98/70/CE, 2009/31/CE, 2009/73/CE, 2010/31/UE, 2012/27/UE e 2013/30/UE del Parlamento europeo e del Consiglio, le direttive del Consiglio 2009/119/CE e 2015/652/UE e che abroga il regolamento 525/2013/UE del Parlamento europeo e del Consiglio.

[22] Regolamento 2018/842/UE del Parlamento europeo e del Consiglio, 30.05.2018, relativo alle riduzioni annuali vincolanti delle emissioni di gas serra a carico degli Stati membri nel periodo 2021-2030 come contributo all'azione per il clima per onorare gli impegni assunti a norma dell'accordo di Parigi e recante modifica del regolamento 525/2013/UE.

[23] Piuttosto consistente è la normativa europea che disciplina il settore dell'energia nella prospettiva della sostenibilità: la Direttiva 2018/2001/UE (RED II, recepita in Italia dal D.Lgs. 8.11.2021 n. 199) sulla promozione dell'uso dell'energia da fonti rinnovabili, la Direttiva 2018/2002/UE sull'efficienza energetica (recepita nell'ordinamento nazionale con il D.Lgs. 14.07.2020, n. 73); la Direttiva 2018/844/UE (*Direttiva Energy Performance of Buildings Directive* – EPBD, recepita in Italia con D.Lgs. 10.06.2020, n. 48 e attualmente affiancata dalla nuova direttiva sulla performance energetica nell'edilizia 2024/1275/UE), che modifica la direttiva 2010/31/UE sulla prestazione energetica nell'edilizia e la direttiva 2012/27/UE sull'efficienza energetica; il Regolamento 2019/941/UE sulla preparazione ai rischi nel settore dell'energia elettrica e il Regolamento 2019/943/UE sul mercato interno dell'energia elettrica; la Direttiva 2019/944/UE relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE ed il Regolamento 2019/942/UE (recepito in Italia con D.Lgs. 8.11. 2021, n. 210) che istituisce un'Agenzia dell'Unione europea per la cooperazione fra i regolatori nazionali dell'energia (ACER).

[24] Ministero dello Sviluppo Economico, Ministero dell'Ambiente e della Tutela del Territorio e del Mare, Ministero delle Infrastrutture e dei Trasporti, Piano Nazionale Integrato per l'Energia e il Clima (PNIEC), dicembre 2019.

[25] Regolamento 2024/1991/UE del Parlamento europeo e del Consiglio, 24.06.2024, sul ripristino della natura e che modifica il Reg. 2022/869/UE.

3.04.2006, n. 152[26]), come il principio di prevenzione *ex* art. 3-*ter*, codice dell'ambiente e il principio di sviluppo sostenibile, di cui all'art. 3-*quater*.

Da ultimo, sugli obiettivi di decarbonizzazione, il Rapporto Draghi del settembre 2024 evidenzia come proprio la decarbonizzazione, insieme, tra l'altro, alla digitalizzazione e all'IA, costituisca una delle maggiori spinte della competitività europea e della sostenibilità ambientale e debba quindi rappresentare una delle priorità dell'azione dell'Unione europea, su cui è opportuno concentrarsi, lasciando altre materie agli ordinamenti nazionali, secondo una più rigorosa applicazione del principio di sussidiarietà[27].

Nel corso degli anni, però, tale concetto di sostenibilità, che sembrava strettamente connesso a quello di tutela ambientale, è stato sempre più esteso, essendo ora inteso come un processo socio-ecologico caratterizzato dal desiderio di perseguire un ideale comune: non solo la tutela dell'ambiente, ma anche della società e dello sviluppo economico, nell'interesse della collettività presente e futura per la tutela di quei diritti dell'uomo e, primi tra tutti, quei diritti già definiti *green rights*.

In questo contesto si sviluppa a livello normativo internazionale ed europee un concetto di sostenibilità con più declinazioni. Di grande rilevanza sul piano internazionale sono i Principi dell'UN *Global Compact*[28], che da tempo invitano le aziende di tutto il mondo ad adottare politiche sostenibili, nel rispetto dei diritti umani, del lavoro, dell'ambiente e nella lotta alla corruzione, in applicazione delle diverse declinazioni della sostenibilità. Si tratta di un'iniziativa di particolare incidenza anche se non sono da escludersi fenomeni di c.d. *Sustainability washing*[29].

Inoltre, con la ratifica dell'*Agenda ONU 2030 per lo Sviluppo Sostenibile*[30], sottoscritta nel settembre 2015 dall'Italia e dai Governi di altri 192 Paesi, la comunità internazionale ha espresso, in maniera netta, un giudizio sull'insostenibilità di un modello di sviluppo fondato solo su obiettivi economici, e che non tenga conto di obiettivi ambientali e sociali. L'Agenda 2030 e i suoi *17 Obiettivi di Sviluppo Sostenibile* (c.d. *Sustainable Development Goals* - SDGs) che ne derivano, costituiscono una grande sfida per i Paesi di tutto

---

[26] D.Lgs. 3.04.2006, n. 152, Norme in materia ambientale (Testo Unico Ambiente – TUA).

[27] M. DRAGHI, *The future of European competitiveness*, Part B, September 2024, 310: *«EU policy and legislative action should refocus on domains where the EU truly has greater added value compared to national or subnational policy action, in line with the subsidiarity principle. Contemporary challenges require collective reflection on where the EU can have greatest added value through collective action, and how to act in these areas in the most efficient and effective way. Examples include ensuring a secure, decarbonised and affordable energy supply under a true Energy Union, or boosting digitalisation and the development, deployment and adoption of advanced digital technologies in the EU – in particular, AI»*.

[28] I dieci principi dell'UN Global Compact sono disponibili sul sito web ufficiale UN *Global Compact* al seguente link: https://www.globalcompactnetwork.org/it/il-global-compact-ita/i-dieci-principi/introduzione/2-i-dieci-principi.html.

[29] Il termine *Sustainability washing* è un'evoluzione del già noto fenomeno del *greewashing* e viene utilizzato con riferimento allo sviluppo di politiche di una sostenibilità di facciata finalizzata ad ingannare le autorità competenti, i fornitori ed i consumatori e modificarne le scelte di acquisto, soprattutto con riferimento ai bilanci di sostenibilità. SI vedano M. ZIOŁO, I. BĄK, A. SPOZ, *Literature review of greenwashing research: State of the art*, in *Corporate Social Responsibility and Environmental Management*, 2024, vol. 31, III, 5343 - 5356, DOI: https://doi.org/10.1002/csr.2842; S.V. DE FREITAS NETTO, M.F. FALCÃO SOBRAL, A.R. BEZERRA RIBEIRO, G.R. DA LUZ SOARES, *Concepts and forms of greenwashing: a systematic review*, in *Environmental Sciences Europe*, 2020, Vol. 32, XIX, 1 – 12, DOI: https://doi.org/10.1186/s12302-020-0300-3.

[30] Gli obiettivi dell'Agenda ONU 2023 sono disponibili sul sito web ufficiale delle Nazioni Unite al seguente link: https://unric.org/it/agenda-2030/.

il mondo. Tali obiettivi rappresentano oggi un punto di riferimento fondamentale per la realizzazione del bilancio di sostenibilità, evoluzione del bilancio sociale, generalmente inteso come *reporting* di natura non finanziaria di carattere volontario.

Piuttosto recenti sono poi le regolamentazioni europee delle politiche sulla sostenibilità nell'ambito della Responsabilità sociale d'impresa (RSI), nota anche con la terminologia inglese *Corporate Social Responsibility* (CSR). In questo contesto emerge la *Corporate Sustainability Reporting Directive* - CSRD (Direttiva 2022/2464/UE, attuata in Italia con il D.Lgs. 6.09.2024, n. 125)[31] sulla rendicontazione di sostenibilità, la quale impone alle società quotate e a quelle di grandi dimensioni l'obbligo di certificazione delle informazioni comunicate sulla sostenibilità, la previsione di requisiti più dettagliati e standardizzati sulle informazioni che le stesse devono comunicare, nonché una migliore accessibilità delle informazioni, imponendone la pubblicazione in una sezione *ad hoc* delle relazioni sulla gestione redatte dalle imprese.

Recentissima è anche la Direttiva sulla *due diligence* aziendale (Direttiva 2024/1760/UE *Corporate Sustainability Due Diligence Directive* - CSDDD[32]), la quale fa seguito alla Risoluzione del Parlamento europeo del 2021 sulla diligenza e la responsabilità delle imprese[33]. Essa, partendo dalla proposta del *Green Deal*, mira a rendere le grandi società europee più responsabili rispetto alle violazioni dei diritti umani e ai danni ambientali per le attività svolte in Europa e al di fuori.

In quest'ottica, hanno iniziato a trovare sempre più applicazione meccanismi di certificazione di ecosostenibilità, anche a partire dalla EU *Taxonomy* (Regolamento 2020/852/UE)[34]. In Italia, il D.L. 31.05.2021, n. 77, conv. in L. 29.07.2021, n. 108, ha emanato le Linee guida per la redazione del progetto di fattibilità tecnica ed economica (PFTE) da porre a base dell'affidamento di contratti pubblici di lavori del PNRR e del PNC[35], volte a definire il contenuto essenziale dei documenti occorrenti alle stazioni appaltanti per l'affidamento, che tengano conto della tassonomia europea.

Ed è in relazione alla tutela della sostenibilità declinata non solo sotto il profilo della tutela ambientale, ma anche sociale ed economica, che acquista sempre più centralità il bilancio di sostenibilità, anche reso secondo i c.d. fattori ESG (*Environmental, Social, Governance*), tanto per il legislatore, che tende a disciplinare in tal senso l'attività delle imprese[36], quanto per le imprese stesse che mirano a improntare le proprie strategie industriali a paradigmi più

[31] Direttiva 2022/2464/UE del Parlamento europeo e del Consiglio, 14.12.2022 che modifica il regolamento 537/2014/UE, la direttiva 2004/109/CE, la direttiva 2006/43/CE e la direttiva 2013/34/UE per quanto riguarda la rendicontazione societaria di sostenibilità (*Corporate Sustainability Reporting Directive* – CSRD).
[32] Direttiva 2024/1760/UE del Parlamento europeo e del Consiglio, 13 giugno 2024, relativa al dovere di diligenza delle imprese ai fini della sostenibilità e che modifica la direttiva 2019/1937/UE e il regolamento 2023/2859/UE (*Corporate Sustainability Due Diligence Directive* - CSDDD).
[33] Risoluzione del Parlamento europeo,10.03.2021 recante raccomandazioni alla Commissione concernenti la dovuta diligenza e la responsabilità delle imprese (2020/2129(INL)).
[34] Regolamento 2020/852/UE del Parlamento europeo e del Consiglio, 18.06.2020 relativo all'istituzione di un quadro che favorisce gli investimenti sostenibili e recante modifica del regolamento (UE) 2019/2088 (*EU Taxonomy*).
[35] Consiglio Superiore dei Lavori Pubblici, Linee guida per la redazione del progetto di fattibilità tecnica ed economica da porre a base dell'affidamento di contratti pubblici di lavori del PNRR e del PNC, luglio 2021.
[36] Per gli obblighi nazionali di predisposizione del bilancio ESG si rinvia al D.lgs. n. 125/2024 di recepimento della Direttiva 2024/2464/UE (CSRD).

moderni e competitivi, anche in risposta a controversie aventi ad oggetto i diritti umani e i cambiamenti climatici[37]. Si tratta di criteri che le aziende possono scegliere di fare propri (tanto con fonti di *hard law* quanto di *soft law*) indirizzando e coordinando l'esercizio della propria attività di impresa verso il rispetto di criteri come l'impegno ambientale, i valori sociali e l'accuratezza e la trasparenza della struttura organizzativa.

I fattori ESG sono ormai dei criteri per la determinazione del punteggio di credito sociale in cui tutte e tre le categorie rappresentate dall'acronimo vengono utilizzate per illustrare la percentuale di rischio di un'azienda per gli investitori e le eventuali parti interessate (*Stakeholders*)[38]. Essi costituiscono, inoltre, criteri di applicazione di norme imperative a tutela dei lavoratori, dell'ambiente o della pubblica amministrazione, da applicare, però, tenendo conto della dimensione e dell'organizzazione dell'azienda.

3. Diritto privato e tutela preventiva della sostenibilità.

La previsione di incentivi e agevolazioni governative mira a orientare le aziende verso uno sviluppo responsabile delle nuove tecnologie. Tuttavia, tali iniziative devono essere affiancate da strumenti normativi di diritto privato per garantire una protezione realmente efficace. Infatti, per rafforzare la tutela preventiva, lo Stato non può fornire da solo gli incentivi sociali ed economici necessari per spingere le aziende a sviluppare *policy* adeguate. Inoltre, anche le agevolazioni statali, come gli sgravi fiscali, devono essere limitate per rimanere sostenibili per la collettività.

In quest'ottica, adeguate qualificazioni e conseguenti classificazioni giuridiche di istituti cardine del diritto privato – come la soggettività giuridica - così come l'adeguamento aziendale alle più innovative strategie di sostenibilità – si pensi alla responsabilità digitale d'impresa ovvero ai contratti verdi applicabili anche nel settore industriale 4.0 – possono essere più concretamente garantiti tramite l'individuazione di determinati strumenti di

[37] Per un approfondimento sui possibili rimedi giuridici *ex post* nell'ambito della responsabilità civile per inquinamento ambientale, mi sia consentito rinviare a M.C. GAETA, *Strumenti di diritto privato per la sostenibilità ambientale nell'industria automobilistica 4.0: un'analisi giuridico-ecodinamica*, in *Actualidad Jurídica Iberoamericana*, XVIII, 2023, 2092 - 2099.

[38] I fattori ESG vengono utilizzati quali criteri per la determinazione del punteggio di credito sociale e prendono in considerazione aspetti specifici racchiusi proprio nell'acronimo ESG. L'aspetto della "E" comprende tutela dell'ambiente e lotta ai cambianti climatici ed è rinvenibile, ad esempio, nell'uso di energia rinnovabile e nella misurazione dell'emissione di gas serra, che è un effetto ambientale diretto prodotto dall'azienda e riguarda l'intero ciclo di vita dell'*hardware* a partire dalla produzione e funzionamento, fino allo smaltimento e riciclaggio di dispositivi e infrastrutture ICT. L'aspetto della "S", invece, è quello dell'impatto sociale, il quale può comprendere dallo *smart working* per il c.d. *work-life balance*, al *digital wellbeing* che consiste nella promozione per forza lavoro, clienti e utenti di un uso responsabile e di un giusto equilibrio nell'utilizzo dei prodotti digitali, al *digital empowerement* a favore di fornitori e dipendenti. Infine, l'aspetto della "G" è incentrato nella gestione dei sistemi tecnologici in chiave anche di *cybersecurity* che, a sua volta, include la *privacy*, con graduazioni e complessità diverse a seconda delle dimensioni e del settore dell'azienda e dei suoi sistemi di tecnologie dell'informazione e della comunicazione – TIC (*Information Communication Technologies* – ICTs). I fattori ESG vengono rendicontati anche nel Bilancio ESG con una lettura finanziaria degli interventi effettuati e di risultati ottenuti; quale esempio applicativo si veda F. LENOCI, *Il Bilancio di Sostenibilità 2023 del Gruppo Cerved concerne Cerved Group S.p.A. e le società consolidate con metodo integrale in coerenza con il Bilancio Consolidato di Gruppo*, in *Amministrazione & Finanza*, 2025, I, III.

diritto privato che garantiscano la tutela dei principi espressamente previsti dalla normativa vincolante, come il principio di prevenzione (art. 3-*ter* TUA) o il principio di sviluppo sostenibile (art. 3-*quater* TUA).

3.1. La qualificazione giuridica della natura nella dicotomia soggetto-oggetto del diritto.

Più specificamente con riguardo agli strumenti di diritto privato per una tutela preventiva della sostenibilità, occorre preliminarmente dare atto di un'annosa questione, che a monte occupa i privatisti, e che è quella della qualificazione giuridica della natura secondo le categorie del diritto privato: ci si interroga, in particolare, sulla corretta classificazione della natura annoverandola tra i soggetti o gli oggetti del diritto, più propriamente, i beni giuridici. Tale qualificazione non si riduce unicamente a un dibattito teorico, ma risulta di fondamentale importanza nella prospettiva di prevenzione, il che rende necessario analizzarla anche in questa sede, sia pur con la dovuta sintesi e rinviando a precedenti scritti sul tema[39]. Infatti, se considerata come soggetto di diritto[40], si dovrebbero attribuire alla natura determinati diritti per garantire una tutela diretta, ma anche doveri e oneri. Al contrario, se si considera la natura quale bene giuridico, allora la sua tutela preventiva risulta incentrata sulla tutela di un'*utilitas* dell'essere umano e anche le attività dei privati devono tenere conto della tutela del bene giuridico-natura, nell'ambito delle proprie *policy* di produzione e sviluppo

La categoria generale della soggettività non può dirsi unitaria, ricomprendendo al suo interno diverse tipologie di entità che vanno dal singolo individuo (persona fisica) alle aggregazioni sociali, formatesi grazie agli interessi comuni dei consociati (enti riconosciuti e non riconosciuti, i primi definiti c.d. persone giuridiche) [41], ma questo non implica la necessità di un'eccessiva estensione della categoria a fattispecie che ben possono essere tutelate come oggetto del diritto.

Nell'esperienza giuridica di stampo civilistico, si definiscono generalmente "oggetto del diritto", tutti i fenomeni sui quali agisce la qualificazione propria del diritto. Secondo un'interpretazione restrittiva, invece, l'oggetto del diritto rappresenta «l'oggetto specifico di una tutela attribuita al soggetto»[42] ed è questo il significato che qui rileva. Sulla base di tale definizione, difatti, la prima caratteristica dell'oggetto del diritto è la sua correlazione logico-pratica con il soggetto del diritto e, precisamente, con il suo interesse. Ciò che costituisce

---

[39] Mi sia consentito rinviare in particolare a M.C. GAETA, *Il problema della tutela giuridica della natura: un'analisi comparata tra Italia e Stati dell'America Latina*, in *NDC*, 2020, IV, 326 - 337, e alla dottrina ivi richiamata.

[40] La nozione di soggetto è il fondamento dell'intera costruzione giuridica, la quale non sarebbe neanche concepibile se non ci fosse un'entità alla quale imputare le situazioni giuridiche soggettive. P. GALLO, *Soggetto di diritto*, in *Dig. civ.*, Torino, 2011, 839.

[41] L. GATT, *Legal anthropocentrism between nature and technology: the new vulnerability of human beings*, in *EJPLT*, 2022, I, 19, DOI: https://doi.org/10.57230/EJPLT221LG, rileva la forte espansione delle categorie giuridiche di soggetto e oggetto di diritto in senso opposto, caratterizzate da confini sempre meno definiti.

[42] Così D. MESSINETTI, *Oggetto dei diritti*, in *Enc. dir.*, XXIX, Milano, 1979, 808 ss.. Secondo l'Autore, infatti, l'oggetto del diritto in senso stretto differisce dagli altri fenomeni giuridici in quanto costituisce il correlato logico e pratico del soggetto. Infatti, come sostenuto chiaramente da P. GROSSI, *I beni: itinerari tra «moderno» e «post-moderno»*, in *Riv. trim. dir. proc. civ.*, 2012, 1060 ss., il bene è sempre un'entità in relazione ad un soggetto.

l'*utilitas* del soggetto si pone come oggetto del diritto[43], che si concretizza nella tutela di un interesse al fine di ottenere il godimento di un bene giuridico. Il bene, quindi, è il bene giuridico tutelato o – come sancisce il codice civile (art. 810 c.c.) – è la cosa immobile[44] o mobile che può essere oggetto di diritti[45].

Ebbene la natura è un insieme di fenomeni e relazioni tra esseri viventi, che possono essere sia soggetti del diritto che beni giuridici. Gli esseri umani sono soggetti di diritto[46], mentre la flora è generalmente considerata bene giuridico[47]. La classificazione della fauna è più complessa: secondo autorevole dottrina, alcune specie animali sarebbero meglio ricollocabili nella categoria dei soggetti di diritto[48]; secondo altri, invece, si tratterebbe di oggetti del diritto[49], seppure senzienti[50].

---

[43] D. MESSINETTI, *op. ult. loc. cit.*, afferma che: «Soggetto-interesse-oggetto sono momenti o aspetti particolari e correlativi di un unitario fenomeno».

[44] Ai sensi dell'art. 812 c.c., sono beni naturali immobili, il suolo, le sorgenti e i corsi d'acqua, gli alberi e tutto ciò che è naturalmente incorporato al suolo.

[45] Per un'approfondita analisi sulla nozione di "beni" cfr. C.M. BIANCA, *Diritto civile*, VI, La proprietà, Milano, 2017, 33 - 84. Recentemente è stato autorevolmente ribadito che l'art. 810 c.c. è una norma di valenza fondante del sistema giuridico italiano e, in generale, la definizione di bene giuridico ha un ruolo centrale in tutti i sistemi giuridici occidentali. Infatti, essendo tutti gli ordinamenti occidentali basati sulla dicotomia soggetto-oggetto del diritto, nel quale non c'è spazio per un terzo genere, la definizione di ciò che viene definito oggetto comporta, *a contrario*, l'identificazione di ciò che non lo è e che, quindi, viene definito soggetto (cfr. L. GATT, *Art. 810*, in *Libro III della proprietà e della famiglia* a cura di L. GATT e S. TROIANO, *Commentario al codice civile diretto da C.M. Bianca*, Roma 2024, 5; EAD., *Legal anthropocentrism between nature and technology*, cit., 17 - 18).

[46] S. COTTA, *Soggetto di diritto*, in *Enc. dir.*, XLII, Milano, 1990, 1214, evidenzia come l'uomo, tanto come individuo («io-soggetto»), che come essere umano, è un soggetto di diritto.

[47] Sulla possibilità di qualificare i beni naturali anche beni comuni, intesi quali beni che non rientrano in senso proprio nella specie dei beni pubblici, potendo appartenere non solo a persone pubbliche, ma anche a soggetti privati ovvero, più frequentemente, a comunità di soggetti che ne usufruiscono v. GATT, *Art. 810*, cit., 7 - 8.

[48] La Dichiarazione Universale dei Diritti dell'Animale, proclamata il 15 ottobre 1978 nella sede dell'Unesco a Parigi, è il primo provvedimento internazionale (anche se privo di un effettivo valore sul piano giuridico) che educa al rispetto di ogni forma di vita. Sulla necessità di ripensare alla categoria giuridica degli animali si veda il volume a cura di S. CASTIGLIONE, L. LOMBARDI VALAURI, *La questione animale*, in *Trattato di Biodiritto*, diretto da S. RODOTÀ, P. ZATTI, I, Milano, 2012, 281 ss. La tesi, inoltre, è autorevolmente sostenuta da L. GATT, L*egal anthropocentrism between nature and technology*, cit., 15 ss., sottolineando la necessità di elaborare delle nuove norme del libro I del nostro codice civile che oggi rileva una profonda inadeguatezza sia nei confronti dell'essere umano che delle altre entità viventi. In particolare, con riferimento agli animali, l'Autrice evidenzia la possibilità di riconoscere una soggettività giuridica ad altri esseri viventi e, nello specifico, agli animali, sottraendoli al raggio applicativo dell'art. 810 c.c. (L. GATT, *Art. 810*, cit., 7). Sul passaggio dalla "considerazione" giuridica degli animali alla loro tutela, nell'ottica di una "giuridificazione" della stessa: G. MARTINI, *Il processo di 'giuridificazione' della protezione degli animali dall'Unità ad oggi*, in AA. VV., *A 150 anni dall'unificazione amministrativa* nazionale, a cura di L. FERRARA, D. SORACE, Vol III, *La Giuridificazione*, a cura di B. MARCHETTI E M. RENNA, Firenze, 2016, 335 - 353; EAD., *La configurabilità della soggettività animale: un possibile esito del processo di 'giuridificazione' dell'interesse alla loro protezione*, *in Riv. crit. dir. priv.*, 2017, I, 109 ss. Nello stesso senso F. RESCIGNO, *Gli esseri animali quali "res senzienti"*, in *Biolaw Journal*, 2019, II, 679 ss.; EAD., *I diritti degli animali. Da res a soggetti*, Milano, 2014. Per una pionieristica analisi sul concetto di ricodificazione del diritto privato si rinvia a U. MATTEI, *Verso una ricodificazione del diritto privato in Italia*, in *Codex: Ideologie e Tecniche della (Ri) Codificazione del Diritto Privato*, *The Cardozo Electronic Law Bulletin Review*, 2019, Vol. 25, I, 1 - 7.

[49] S. COTTA, *Soggetto di diritto*, cit., 1215, definisce gli animali, i beni naturali e gli eventi naturalistici in generale (es. *insula in flumine nata*) come oggetti del diritto in quanto non sono autori. Allo stesso modo, l'Autore ritiene che i diritti degli animali siano quelli che l'uomo attribuisce loro in quanto oggetti di diritto e non soggetti attivi titolari di diritti.

[50] L'Unione europea ha esplicitamente riconosciuto gli animali quali «esseri senzienti» all'articolo 13 del Trattato di Lisbona del 2007, comprendendo anche una dimensione morale, in quanto gli animali sono dotati di sensibilità e sono in grado di provare sofferenza e dolore. Sugli stessi principi si basa anche la Convenzione europea per la protezione degli animali da compagnia, firmata a Strasburgo il 13.1.1987 e ratificata dall'Italia con la legge 4.11.2010, n. 210. A tale Convenzione ha fatto seguito l'Accordo del 6 febbraio 2003, che

Negli ultimi anni assistiamo a numerosi casi di dilatazione della soggettività giuridica, a partire proprio dalla natura in alcune sue manifestazioni, come nei casi decisi dalla Corte Suprema della Colombia nel 2016, in merito alla soggettività giuridica del Rio Atrato[51] e nel 2018 sulla soggettività giuridica della foresta amazzonica[52]. Più recente, appena nel novembre 2024, poi, è il caso del riconoscimento della soggettività giuridica al Mar Menor, deciso dal Tribunale costituzionale spagnolo confermando la legge spagnola n. 19/2022[53]. Oltre alla natura, un altro esempio significativo di ampliamento interpretativo della soggettività giuridica è rappresentato dalla robotica alla quale pure si è ipotizzato di attribuire una personalità elettronica[54]. Ma come per la natura,

definisce alcuni principi fondamentali per una maggiore e più corretta relazione tra l'uomo e gli animali da compagnia, siglato in sede di Conferenza Stato Regioni, tra il Ministero della Salute, le Regioni e le Province autonome di Trento e Bolzano e recepito con d.P.C.M. 28 febbraio 2003. Va almeno menzionata, infine, la legge quadro in materia di tutela degli animali d'affezione e lotta al randagismo del 14.08.1991, n. 281, che favorisce la corretta convivenza tra uomo e animale e tutela la salute pubblica e l'ambiente.

[51] Si veda, in particolare, la decisione resa nel caso del rio Atrato, con cui la Corte Suprema colombiana ha riconosciuto il «*río Atrato, su cuenca y afluentes como una entidad sujeto de derechos*» e ha imposto allo Stato di proteggere e far rivivere il fiume e i suoi affluenti, dando allo Stato sei mesi di tempo per la cessazione delle attività minerarie inquinanti, bonificare il territorio e indennizzare le comunità etniche indigene per danni provocati dallo sfruttamento non sostenibile del bacino fluviale (cfr. Corte Suprema della Repubblica di Colombia, sent. 10 novembre 2016, T-622/2016). Le attività attualmente intraprese per attuare il disposto della sentenza della Corte sono disponibili sul sito web del Ministero dell'ambiente e dello sviluppo sostenibile colombiano al seguente link: https://archivo.minambiente.gov.co/index.php/component/content/article/130-notas-de-interes/3386-actividades-para-el-cumplimiento-de-la-sentencia-t-622-que-reconoce-al-rio-atrato-como-sujeto-de-derechos.

[52] Il Tribunale Supremo della Colombia ha riconosciuto la Foresta Amazzonica come entità, «soggetto di diritti», il che significa che la foresta pluviale è stata annoverata tra i soggetti di diritto e le sono stati concessi gli stessi diritti di una persona fisica, tra cui proprio quello alla vita, e il dovere di tutelarla incombe sui governi e sugli enti locali dell'Amazzonia (cfr. Corte Suprema della Repubblica di Colombia, sentenza 5 aprile 2018, n. 4360, punto 14: «*Por tanto, en aras de proteger ese ecosistema vital para el devenir global, tal como la Corte Constitucional declaró al rio Atrato, se reconoce a la Amazonia Colombiana como entidad, "sujeto de derechos", titular de protección, conservación, mantenimiento y restauración a cargo del Estado y las entidades territoriales que la integran*»).

[53] È recentissima la decisione con cui il Tribunale costituzionale spagnolo, confermando la legittimità costituzionale della legge 30.09.2022, n. 19 che riconosceva personalità giuridica alla laguna del Mar Menor e al suo bacino, ha ritenuto così di rafforzare la tutela dell'ambiente e, con essa, la dignità umana, dal momento che «*la vida digna solo es posible en entornos naturales idóneos, y ello desde la consideración de la vida de las generaciones actuales y de la vida de las generaciones futuras*»; con la legge ritenuta legittima si verifica così «*un traslado de paradigma de protección desde el antropocentrismo más tradicional, a un ecocentrismo moderado*». Il contenuto della sentenza è stato anticipato dal quotidiano *El País*, che ha avuto accesso al testo (cfr. J.M. BRUNET, *El Constitucional avala que el mar Menor goce de personalidad jurídica para su mayor protección*, in *El País*, 20.11.2024, accessibile al seguente link: https://elpais.com/clima-y-medio-ambiente/2024-11-20/el-constitucional-avala-que-el-mar-menor-goce-de-personalidad-juridica-para-su-mayor-proteccion.html), oltre che dal comunicato stampa n. 115/2024 dello stesso *Tribunal Constitucional,* accessibile al seguente link: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2024_115/NOTA%20INFORMATIVA%20Nº%20115-2024.pdf. Come si legge nel comunicato stampa, la sentenza riconosce che la legge n. 19/2022 è una regolamentazione unica nel suo genere per l'ordinamento giuridico spagnolo, in quanto crea una nuova tipologia di persona giuridica, una realtà naturale, al fine di dotarla di una serie di diritti specifici, legati proprio alla tutela ambientale. Si tratta di una tecnica normativa nuova per il diritto ambientale spagnolo, la quale si inserisce in un movimento internazionale in crescita nell'ultimo decennio, che promuove il riconoscimento dei c.d. diritti della natura.

[54] Risoluzione del Parlamento europeo recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, del 16.02.2017, principio n. 59 lett f). Per un commento critico mi sia consentito rinviare a, M.C. GAETA, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies*, Napoli, 2019 (Ris. 2023), 55 - 56.

neanche per la robotica né per l'IA appare opportuno riconoscere uno *status* giuridico di soggetto di diritto[55].

Coerente con tale classificazione della natura quale bene giuridico è la riforma della tutela dell'ambiente nella costituzione italiana, che con l'introduzione di un nuovo co. 3 all'art. 9 Cost. ha innalzato a principio costituzionale quello della tutela dell'ambiente, della biodiversità e degli ecosistemi, anche nell'interesse delle generazioni future, ed ha attribuito allo Stato l'individuazione dei modi e delle forme di tutela degli animali[56]. L'art. 41 Cost., poi, prevede ora espressamente quale limite alla libertà dell'iniziativa economica privata la necessità che non sia arrecato danno non solo all'essere umano (sicurezza, libertà, dignità), come era già previsto, ma adesso anche alla sua salute e all'ambiente quali diritti dell'uomo[57]. La tutela del bene giuridico "ambiente", quindi, è strumentale per la tutela dei diritti dell'uomo.

3.2. Responsabilità digitale d'impresa e meccanismi di misurazione.

La previsione di strumenti preventivi per la sostenibilità ha una funzione particolarmente rilevante se applicata all'ambito industriale, soprattutto per quelle realtà aziendali che utilizzano le più innovative applicazioni tecnologiche di IA, tanto nel processo di produzione, quanto nei servizi e prodotti finali che immettono sul mercato. I meccanismi produttivi incentrati su innovative tecnologie, infatti, comportano il rischio di un aumento dell'inquinamento ambientale, causato da sistemi di produzione tecnologici, che possono risultare più rapidi e performanti, ma anche più inquinanti, oltre che economicamente più gravosi. Inoltre, tali tecnologie possono avere un forte impatto anche sul piano sociale, portando allo sfruttamento di alcune comunità più disagiate per l'estrazione delle materie prime necessarie per le nuove fonti di energia (si pensi all'estrazione del litio nelle miniere in Cile o in alcuni paesi africani come lo Zimbabwe e la Namibia). Allo stesso tempo, i prodotti finali, e nel caso di specie quelli intelligenti, rischierebbero di essere meno inquinanti nel breve periodo, ma paradossalmente molto più inquinanti sul lungo periodo (si pensi ad esempio alle difficoltà per lo smaltimento delle batterie a litio). Pertanto, una *governance* aziendale fondata su innovativi criteri sociali di *compliance by design e by default* [58] , che integrino anche quelli di sostenibilità, può

[55] L. GATT, *Legal anthropocentrism between nature and technology*, cit., 21 - 25, sostiene l'esigenza di un miglioramento dello *status* giuridico di alcune forme di esseri viventi, come il già menzionato caso degli animali - in quanto esseri senzienti - e dell'embrione umano - in quanto prima forma di vita dell'essere umano - che potrebbero essere più opportunamente tutelati quali soggetti di diritto. Sulla soggettività giuridica dell'embrione umano con particolare riguardo all'identità genetica, si rinvia a L. GATT, *Il problema dei minori senza identità genetica nei (vecchi e) nuovi modelli di famiglia: il conflitto tra ordine pubblico interno e c.d. ordine pubblico internazionale*, in *Familia*, 2017, II, 272; sulla dialettica tra soggetto e oggetto di diritto con riguardo all'ovulo, al gamete, e all'embrione v. EAD., *Art. 810*, cit., 6-7. In merito alla soggettività giuridica dei robot, invece, dubbi vengono posti anche dall'Autrice (EAD., *Art. 810*, cit., 8).

[56] Per un approfondimento sulla riforma dell'art. 9 Cost., con particolare riguardo all'affidamento alla legge statale della disciplina della tutela degli animali e alla possibile configurabilità di una soggettività animale, si rinvia a G. MARTINI, *L'impervio percorso della soggettività animale*, in *BioLaw Journal*, 2022, IV, 355 - 384.

[57] Per una più dettagliata analisi della riforma costituzionale e della qualificazione giuridica della natura in Italia, mi sia consentito rinviare a M.C. GAETA, *Il problema della tutela giuridica della natura* cit., 326 - 330.

[58] Per *compliance by design e by default* si fa riferimento all'insieme di processi e procedure (inclusa la progettazione e implementazione di software tecnologici di IA per la produzione o da produrre per immetterli sul mercato) che un'azienda sviluppa per assicurarsi di rispettare leggi, regolamenti e normative applicabili al suo settore di attività. Tale organizzazione aziendale va prevista sin dalla fase iniziale della

rappresentare un punto di forza per la tutela degli individui e del pianeta, cui gli stessi appartengono.

Nell'ambito della già menzionata RSI, la recente regolamentazione europea (EU *Taxonomy*, CSRD e CSDDD) costituisce già un evidente passo avanti nella prospettiva della sostenibilità aziendale per la tutela dei diritti umani a cominciare proprio dai *green rights*. Tuttavia, in conseguenza dello sviluppo tecnologico e delle nuove esigenze di *compliance* sempre più incentrate su tali tecnologie, la RSI viene ripensata e si sviluppa la Responsabilità digitale d'impresa – RDI (*Corporate Digital Responsibility* - CDR)[59], la quale mira in primo luogo a garantire un impegno delle aziende verso l'adozione di pratiche digitali che siano etiche, eque e tutelino la *privacy*[60]. Tale ambito di applicabilità della RDI si interseca sempre più con il concetto della sostenibilità intesa a tutto tondo[61] e ha un impatto significativo sulle strategie dell'IA, influenzando vari aspetti operativi e decisionali delle organizzazioni, come efficienza energetica e riduzione delle emissioni, economia circolare e gestione dei rifiuti tecnologici, nonché sviluppo di *software* sostenibili, trasparenza nell'utilizzo e gestione dei dati, predisposizione di nuove tecniche di *smart-working* e *coworking*. La RDI, infatti, non può più limitarsi a considerare le nuove tecnologie (soprattutto quelle di IA) come semplice fattore abilitante della organizzazione o dei modelli aziendali, ma deve soppesare l'impatto ambientale, sociale e ed economico nelle sue modalità applicative, esplicate nella rendicontazione di sostenibilità (nel bilancio di sostenibilità o proprio nel bilancio ESG), divenendo così il volano anche per l'implementazione dei fattori ESG nelle aziende, sin dalla fase di progettazione, e fino a quella di gestione dei sistemi basati su IA, intesi quale prodotto dell'attività aziendale, ma anche come strumento per lo sviluppo della stessa.

---

pianificazione produttiva (*by design*), tanto manuale quanto automatizzata, nonché per impostazione predefinita (*by default*) verificando, così, l'attuazione di tali processi/procedure. Si tratta di policy per ora sviluppate in determinati contesti, come quello della *privacy* o del settore bancario, ma di cui si percepisce l'esigenza – a livelli diversi – in tutti i contesti aziendali. Con riguardo alla *compliance* aziendale, si pensi ad esempio all'analisi Pest (*Political, Economic, Tocial e Technological*) e alla più recete analisi Pestle (*Political, Economic, Social, Technological, Legal e Environmental*): A. QUARANTA, *Cosa sono le analisi PEST e PESTLE, e quanto possono essere utili per comprendere i fattori esterni che influenzano il contesto, sempre più complesso, in cui operano le aziende?*, in *Ambiente & Sviluppo*, 2024, XII, 859 ss.; invece, sui sistemi intelligenti prodotti in relazione alle tecnologie di *Brain Computer interface* (BCI), si rinvia a L. GATT, I.A. CAGGIANO, M.C. GAETA, A.A. MOLLO, *BCI devices and their legal compliance: A prototype tool for its evaluation and measurement*, in *EJPLT*, 2022, I, 301 - 314, DOI: https://doi.org/10.57230/EJPLT221LGIACMCGAAM.

[59] Per un approfondimento sulla *Corporate Digital Responsibility* si rinvia a K.V. CARL, T. ZILCHER, O. HINZ, *Corporate Digital Responsibility and the current Corporate Social Responsibility standard: An analysis of applicability*, in *Open Identity Summit*, Copenhagen, 2022, 75-86, DOI: https://doi.org/10.18420/OID2022_06; K.V. CARL, C. MIHALE-WILSON, J. ZIBUSCHKA, O. HINZ, *A consumer perspective on Corporate Digital Responsibility: an empirical evaluation of consumer preferences*, in *Journal of Business Economics*, Vol. 94, 2023, 979-1024; L. LOBSCHAT, B. MUELLER, F. EGGERS, L. et al., *Corporate digital responsibility*, in *Journal of Business Research*, Vol. 122, 2021, 875 - 888, DOI: https://doi.org/10.1016/j.jbusres.2019.10.006.

[60] Sulla protezione dei dati personali e la sostenibilità ambientale nei diritto contrattuale si rinvia a I.A. CAGGIANO, *Modelli negoziali di condivisione di dati: prospettive applicative e la sostenibilità ambientale*, in A.A. VV., *Dalla Data Protection alla Data Governance: il regolamento (UE) 2022/868 Commentario al Data Governance Act,* a cura di A. MORACE PINELLI, Pisa, 2024, 83 - 106.

[61] Sull'estensione della RDI all'ambito della sostenibilità si vedano: J. WIRTZ, W.H. KUNZ, N. HARTLEY, J. TARBIT, *Corporate digital responsibility in service firms and their ecosystems*, in *Journal of Service Research*, Vol. 26, II, 2022, 173-190, DOI: https://doi.org/10.1177/10946705221130467; C.J. HERDEN, E. ALLIU, A. CAKICI, et al., *Corporate Digital Responsibility*, in Nachhaltigkeits Management Forum, 2021, Vol. 29, 13 - 29, DOI: https://doi.org/10.1007/s00550-020-00509-x.

Nell'ambito delle pratiche aziendali connesse alla RDI delle industrie del settore IA, sono sempre più centrali quelle che consentono di misurare il livello di sostenibilità dei sistemi di IA prodotti e più in generale l'impatto del potenziale rischio di tali sistemi; e tali pratiche si sviluppano, in linea con le *policy* e le normative sovranazionali e nazionali.

Lo stato dell'arte dell'impatto dei sistemi di IA sui diritti umani parte dall'analisi delle carte dei diritti fondamentali internazionali ed europei[62], per poi rivestire grande rilevanza nella recentissima Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto del 2024[63]. La Convenzione quadro formula principi e regole fondamentali da rispettare nell'ambito del ciclo di vita dei sistemi di IA per la tutela anche di quei diritti sopramenzionati, già definiti *green rights*, tra i quali: dignità umana, uguaglianza e non discriminazione, salute, protezione dell'ambiente e *privacy*.

Per quanto riguarda il livello dell'UE, la più recente normativa di diritto interno sull'IA è il Regolamento sull'IA, il già menzionato AI Act, che fa parte di un più ampio sistema di misure politiche a sostegno dello sviluppo di un'IA affidabile, che comprende anche il Pacchetto Innovazione IA [64] e il Piano coordinato sull'IA[65]. Insieme, queste regolamentazioni mirano a garantire la sicurezza delle tecnologie dell'IA e la protezione dei diritti fondamentali degli individui e delle imprese in relazione alle applicazioni dell'IA. Inoltre, tali iniziative puntano a rafforzare gli investimenti e l'innovazione nell'IA in tutta l'UE.

Anche da un punto di vista etico, poi, emerge la necessità di verificare l'impatto dell'IA sugli individui e sulla realtà sociale in generale[66], nonché, più nello specifico, sulla società, sulla psicologia umana (segnatamente sulla

[62] Quanto alle carte dei diritti fondamentali, particolarmente rilevanti sono, a livello europeo, la Carta dei diritti fondamentali dell'Unione europea (CDFUE) del 7.12.2000, mentre, a livello internazionale la Dichiarazione universale dei diritti dell'uomo (UDHR) del 10.12.1948 e la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) del 4.11.1950.

[63] Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto del 5.09.2024. L'Ad Hoc Committee on AI (CAHAI) del Consiglio d'Europa, ha elaborato in collaborazione con l'Alan Turing Institute del Regno Unito tra il 2019 e il 2021 un modello uniforme per *la human rights impact assessments of AI systems* (HRIAs), attualmente conforme alla Convenzione Quadro del Consiglio d'Europa sull'IA e che prende il nome di HUDERIA (*Human Rights, Democracy, and the Rule of Law Impact Assessment*). Il modello è stato adottato dal Consiglio d'Europa nel novembre 2024. Per un approfondimento si veda: Ad Hoc Committee on AI (CAHAI) del Consiglio d'Europa, *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), 28.11.2024, CAI(2024)16rev2, accessibile al seguente link: https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f

[64] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sulla promozione delle start-up e dell'innovazione nell'intelligenza artificiale affidabile*, 24.01.2024, COM(2024) 28 final; per un quadro generale sul pacchetto di iniziative europee per sostenere le start-up e le PMI nello sviluppo di un'intelligenza artificiale (IA) affidabile si veda la pagina web ufficiale della Commissione europea, *La Commissione vara un pacchetto per l'innovazione in materia di IA a sostegno delle start-up e delle PMI nel settore dell'intelligenza artificiale*, https://ec.europa.eu/commission/presscorner/detail/it/ip_24_383.

[65] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Piano coordinato sull'intelligenza artificiale*, 7.12.2018, COM(2018) 795 final. Per una panoramica sul Piano di coordinamento dell'IA e per i suoi aggiornamenti si veda anche la pagina web ufficiale della Commissione europea, Piano coordinato sull'intelligenza artificiale, https://digital-strategy.ec.europa.eu/it/policies/plan-ai.

[66] Studio del Parlamento europeo, *Artificial intelligence: From ethics to policy*, PE641.507, giugno 2020.

fiducia), sui sistemi finanziari, sull'ambiente, rilevata tanto in studi europei[67] quanto in atti di *soft law*[68].

La verifica dell'impatto dell'IA è un'analisi dei rischi che la stessa può comportare per gli individui e i propri diritti, la quale implica concretamente una misurazione di tali rischi sulla base di una determinata scala di valori. Essa, quindi, costituisce l'evoluzione del concetto di misurazione, analizzato anche dal punto di vista giuridico[69]. È in questo contesto che si è sviluppato l'IA Act, che evidenzia l'impiego di una metodologia basata sull'analisi del rischio e prevede che i sistemi di IA ad alto rischio debbano essere valutati, in fase preventiva e monitorati per tutto il loro ciclo di vita, attraverso uno strumento di gestione del rischio che tali sistemi di IA possono produrre (art. 9 AIA), nonché una valutazione dell'impatto di determinati sistemi di IA ad alto rischio sui diritti fondamentali, in applicazione di quanto previsto dall'art. 27 AIA[70].

Con specifico riferimento alla metodologia dell'approccio basato sull'analisi rischio (*risk based approach*) e, più in particolare, alla valutazione dell'impatto del rischio (*risk impact assessment*), sembra opportuno evidenziare che, negli ultimi anni, l'Unione europea ha fondato i propri atti normativi di *hard law* sull'analisi dell'impatto del rischio di un prodotto/servizio sui diritti umani, dalla fase di progettazione fino all'introduzione sul mercato e al relativo utilizzo. Un classico esempio è quello rappresentato dalla valutazione d'impatto sulla protezione dei dati, nota come *Data Protection Impact Assessment* - DPIA (art. 35 Reg. 2016/679/UE - GDPR)[71], seguito poi anche dalla valutazione del rischio sui diritti umani derivante dalla progettazione e dal funzionamento delle

---

[67] Studio del Parlamento europeo, *The ethics of artificial intelligence: issues and initiatives*, PE 634.452, marzo 2020; Studio del Parlamento europeo, *European framework on ethical aspects of artificial intelligence, robotics and related technologies*, PE 654.179, Settembre 2020.

[68] Gli atti di *soft law* che evidenziano la necessità di garantire un'IA affidabile provengono dal Parlamento europeo, dalla Commissione europea e dal Gruppo di esperti sull'IA nominato dalla Commissione UE nel 2019 (*High-level Expert Group on Artificial Intelligence*). In particolare, quanto alle istituzioni europee, si vedano: Risoluzione del Parlamento europeo, *Framework of ethical aspects of artificial intelligence, robotics and related technologies*, 20.10.2020, PROV(2020)0275; White Paper della Commissione europea *on Artificial Intelligence – A European Approach to Excellence and Trust*, 19.02.2020, COM(2020)65 final; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Creare fiducia nell'intelligenza artificiale antropocentrica*, 8.04.2019, COM(2019)168 final. Sui lavori del gruppo europeo di esperti in tema di IA si rinvia all'HLEG-AI, *The Assessment List for Trustworthy Artificial Intelligence* (ALTAI), 17.07.2020, il quale è il risultato di studi svolti il precedente anno dallo stesso gruppo di esperti: HLEG-AI, *Policy and investment recommendation for trustworthy AI*, 26.06.2019; HLEG-AI, *A definition on AI: Main capabilities and Disciplines*, 8.04.2019; HLEG-AI, *Ethical Guidelines for Trusted AI*, 8.04.2019.

[69] Per una prima analisi del concetto di misurazione in relazione alle tecnologie di *Brain Computer interface* (BCI), si rinvia a L. GATT, I.A. CAGGIANO, M.C. GAETA, E. TROISI, R. SAVELLA, F. PRATESI, R. TRASARTI, *FRIA implementation model according to the AI Act*, in *IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering* (MetroXRAINE), 2024, (in corso di pubblicazione).

[70] S. BERTAINA, I. BIGANZOLI, R. DESIANTE et al, *Fundamental Rights and Artificial Intelligence Impact Assessment: A New Quantitative Methodology in the Upcoming Era of Ai Act*, 2024, DOI: http://dx.doi.org/10.2139/ssrn.4698609; A. MANTELERO, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in* AI, Torino, 2022, 45 – 54; H. JANSSEN, M.S. AH LEE, J. SINGH, *Practical fundamental rights impact assessments*, in *International Journal of Law and Information Technology*, 2022, Vol. 30, II, 200 - 232, DOI: https://doi.org/10.1093/ijlit/eaac018; A. MANTELERO, S.M. ESPOSITO, *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, in *Computer Law & Security Review*, 2021, Vol. 41, DOI: https://doi.org/10.1016/j.clsr.2021.105561.

[71] Regolamento del Parlamento europeo e del Consiglio, 2016/679/UE, 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – *General Data Protection Regulation*, in sigla GDPR).

piattaforme online e dei motori di ricerca online di grandi dimensioni (art. 34 Reg. 2022/2065/UE - DSA) [72] , con esplicito riferimento anche ai diritti fondamentali (art. 34, comma 1, lett. b, DSA)[73].

A livello italiano, il concetto di misurazione e verifica dell'impatto dell'IA emergeva già nel Libro Bianco dell'Agenzia per l'Italia Digitale (AgiD) del 2018. In particolare, la sfida era incentrata sulla misurazione dell'impatto delle soluzioni di IA implementate nella attività della pubblica amministrazione[74]. Il Libro Bianco, nello specifico, affrontava il tema da due punti di vista: quello dei cittadini (qualità della vita delle persone e *customer satisfaction*) e quello delle istituzioni (ottimizzazione dei processi organizzativi), sottolineando la necessità di valutare l'impatto delle tecnologie di IA tramite un approccio multidisciplinare alla misurazione del rischio, con l'obiettivo di progettare e sviluppare un'IA affidabile e trasparente, per ridurre il rischio di errori (e quindi di possibili danni all'individuo).

Nel 2024, il concetto di "impatto", seppur in senso più ampio, viene ripreso, anche nella Strategia Italiana per l'Intelligenza Artificiale 2024-2026 dell'AgID[75] con riferimento alla ricerca scientifica, alla pubblica amministrazione, alle imprese e all'istruzione. In particolare, emerge la necessità di potenziare la ricerca applicata all'Intelligenza Artificiale, attraverso iniziative co-progettate da partenariati pubblico-privati, focalizzandosi su contesti di maggior valore economico e sociale per l'Italia e di maggior impatto sul benessere dei cittadini. Inoltre, la strategia evidenzia la necessità di rendere più efficienti i processi della pubblica amministrazione, con un focus specifico su aree di intervento ben delineate da parte della pubblica amministrazione, anche in considerazione dell'impatto e dei rischi dei sistemi di IA.

Sul piano del diritto cogente, poi, nel maggio 2024, il Consiglio dei Ministri italiano ha approvato il disegno di legge italiano sull'IA[76]. Si tratta di un testo in linea con l'AI Act eurounitario ed effettivamente non poteva che essere così in considerazione della impossibilità di prevedere regolamentazioni solo nazionali per un fenomeno mondiale, senza confini. Il DDL promuove, infatti, l'uso corretto, trasparente e responsabile dei sistemi di IA, in una dimensione antropocentrica, nonché garantendo la vigilanza e la gestione dei rischi economici e sociali e, nello specifico, l'impatto dell'IA sui diritti fondamentali (art. 1). Tuttavia, il disegno di legge disciplina anche alcuni aspetti di interesse

[72] Regolamento del Parlamento europeo e del Consiglio 2022/2065/UE, 19.10.2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali – *Digital Services Act*, in sigla DSA).

[73] A. MANTELERO, *Fundamental Rights Impact Assessment in the DSA*, in AA.VV., *Putting the DSA into practice*, a cura di J. VAN HOBOKEN, J.P. QUINTAIS, N. APPELMAN, R. FAHY, I. BURI, M. STRAUB, Berlino, 2023, 109 - 117.

[74] Libro Bianco dell'Agenzia per l'Italia Digitale (AgID), *L'Intelligenza Artificiale al servizio del cittadino,* marzo 2018, Sfida n. 8.

[75] Agenzia per l'Italia Digitale (AgID), Strategia Italiana per l'intelligenza artificiale 2024-2026, aprile 2024, 4 - 12.

[76] DDL n. 1146/2024 Disposizioni e delega al Governo in materia di intelligenza artificiale (Titolo breve: Intelligenza artificiale), presentato su iniziativa governativa i 20.05.2024 e annunciato nella seduta del 21.05.2024 n. 191, assegnato alle commissioni riunite 8ª (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) e 10ª (Affari sociali, sanità, lavoro pubblico e privato, previdenza sociale) in sede referente il 29.05.2024 e annuncio lo stesso giorno nella seduta n. 195. Dal 27.11.2024 il DDL è in corso di esame in commissione. Maggiori informazioni sull'*iter* legislativo sono disponibili sulla relativa pagina del sito web del Senato della Repubblica: https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm.

principalmente nazionale, come i principi della sperimentazione, della ricerca, dello sviluppo, dell'adozione e dell'applicazione dei sistemi di IA, intervenendo in cinque aree specifiche: strategia nazionale, autorità nazionali, azioni di promozione, protezione del *copyright* e sanzioni penali. Gli aspetti di applicazione nazionale risultano essere tra quelli di maggiore rilevanza del DDL, dal momento che per il resto la disciplina nazionale si è posta in linea con quella europea dell'AI Act, direttamente applicabile, integrandola solo per quanto necessario.

Appare evidente, quindi, che i metodi della misurazione e dell'analisi dell'impatto del rischio sono sempre più centrali per le istituzioni e iniziano ad essere recepiti anche a livello aziendale. Ciononostante, oltre ad emergere punti di forza di tale nuovo approccio, si rilevano non poche criticità. Ad esempio, i meccanismi di misurazione e verifica RDI si fondano su sistemi di autovalutazione (*self-assessment*) che, sebbene di per sé possano rappresentare uno strumento di tutela preventiva in grado di garantire un migliore livello di sostenibilità aziendale, in realtà possono celare un rischio di discrezionalità e strumentalizzazione[77]. Ecco perché sono sempre più centrali i meccanismi di certificazione di sostenibilità fondati sui già menzionati fattori ESG e ciò vale ancor di più per le realtà aziendali quotate, o comunque di grandi dimensioni, che utilizzano e/o producono tecnologie avanzate, come quelle di IA. Si tratta, infatti, di certificazioni basate su fattori oggettivamente considerati e ottenuti a seguito di valutazioni effettuate da terzi, anche se soggetti privati e spesso dopo un primo questionario compilato dal diretto interessato[78].

3.3. Contratti d'impresa a garanzia della sostenibilità dell'intelligenza artificiale.

La crescente importanza che le tematiche della sostenibilità hanno assunto negli ultimi anni ha reso necessaria l'adozione di misure specifiche da parte delle aziende per ridurre l'impatto delle proprie attività. Ciò è di particolare rilevanza per le aziende 4.0, le quali hanno iniziato a rispondere alla pressione esercitata dal mercato, dalla società civile e, in alcuni casi, anche già dal

[77] È il caso, ad esempio, del celebre scandalo Volkswagen (c.d. *Dieselgate* del 2015), emblematico esempio di *greenwashing*[77], che aveva visto dichiarati dei livelli di emissioni inquinanti inferiori risetto a quelli reali. Per un approfondimento si rinvia F. BERTELLI, Profili civilistici del «*dieselgate*». Questioni risolte e tensioni irrisolte tra mercato e sostenibilità, Napoli, 20211, 135 - 145.

[78] Tra i sistemi privati di autocertificazione in merito al livello di *compliance* aziendale ESG, si menziona EcoVadis (www.ecovadis.com), una delle più importanti piattaforme internazionali di rating che si occupa di misurare il livello di *compliance* rispetto ai fattori ESG, misurando la qualità del sistema di gestione della sostenibilità di un'azienda attraverso le sue politiche, azioni e risultati. Il modello di valutazione, che si basa su standard riconosciuti a livello mondiale come GRI (*Global Reporting Initiative*), UNGC (Patto Mondiale delle Nazioni unite), ISO 26000, e che è presidiato da un comitato scientifico internazionale, consiste nel verificare, attraverso un questionario, le performance del fornitore in relazione a quattro macro-ambiti: ambiente; pratiche lavorative e Diritti Umani; etica; approvvigionamento sostenibile. Il punteggio per ogni settore si basa sulle prestazioni dell'azienda in base a sette indicatori di gestione, mentre il punteggio complessivo è dato dalla media ponderata dei risultati nei quattro ambiti. Inoltre, il punteggio tiene conto dei fattori di rischio legati alle dimensioni e al Paese, che EcoVadis rivede e rielabora regolarmente per riflettere l'ampia gamma di fattori di rischio.

legislatore[79], predisponendo *policy* aziendali di compliance *by design* e *by default* fondate sulle diverse declinazioni del concetto di sostenibilità. Lo scopo di tali iniziative è quello di risultare, così, maggiormente competitive nelle contrattazioni, sia pubbliche che private. Difatti, i contratti aziendali possono favorire il raggiungimento di più elevati obiettivi di sostenibilità, non soltanto per quanto riguarda la contrattualistica pubblica - già piuttosto sviluppata nel settore *green*[80] - ma anche nei rapporti tra privati, anch'essi sempre più incentrati sulla evidente necessità di preservare le risorse naturali[81].

La sostenibilità ambientale, quindi, è ormai elemento preferenziale ai fini dell'aggiudicazione di appalti pubblici, ed anche nell'ambito del diritto privato le imprese e i consumatori possono cogliere le maggiori opportunità di crescita collegate alla transizione ecologica, inserendo nei contratti clausole "verdi" di diversa natura[82]. Impostare la politica industriale in un'ottica di ecosostenibilità consente alle aziende stesse di essere preferite nelle relazioni con la pubblica amministrazione (partecipare a un maggior numero di appalti pubblici, come già sperimentato in molti di quelli legati all'attuazione del PNRR) e con i privati. Si tratta di assumere una prospettiva ecologica, a diversi livelli della filiera produttiva, che implica l'adozione di criteri ormai di rilevanza economica[83]. È per queste ragioni che anche tra privati si stipulano sempre più spesso contratti verdi o «contratti ecologici»[84], ispirati a criteri di sostenibilità talvolta persino

---

[79] Si vedano, ad esempio, la Direttiva 2022/2464/UE (CSRD) sulla rendicontazione di sostenibilità e la Direttiva 2024/1760/UE (CSDDD) sugli obblighi di diligenza per le aziende in termini di sostenibilità, già richiamate.

[80] Cfr. S. COLOMBARI, *Le considerazioni ambientali nell'aggiudicazione delle concessioni e degli appalti pubblici*, in *Urbanistica e appalti*, 2019, I, 5 ss., che rileva come le esigenze ambientali nell'ambito delle concessioni e degli appalti pubblici siano fondate sul graduale affermarsi del principio di integrazione funzionale allo sviluppo sostenibile, prima a livello europeo e, poi, anche nazionale: in quest'ottica, si assiste già a partire dal Codice dei contratti pubblici del 2016 (d.lgs. 50/2016) a un'ulteriore valorizzazione dei criteri di sostenibilità ai fini dell'aggiudicazione dei contratti pubblici, in quanto gli stessi divengono uno strumento determinante ai fini della transizione verso un'economia circolare.

[81] M. PENNASILICO, *Le categorie del diritto civile tra metodo e storia (a proposito del libro di Nicola Lipari)*, in *Riv. Dir. Civ.*, 2016, V, 1246 ss., secondo cui «*L'interesse ambientale, che per lungo tempo ha costituito un vincolo esterno alle procedure a evidenza pubblica, poiché l'originaria normativa comunitaria rispondeva al solo interesse economico della tutela della concorrenza, può considerarsi oggi un dato immanente o un vincolo interno alle procedure tanto di affidamento dei contratti pubblici quanto di formazione di qualsiasi "contratto ecologico", anche di diritto privato, purché fonte di rapporti patrimoniali "sostenibili"*». Cfr. anche ID.: *Contratto e uso responsabile delle risorse naturali*, in *Rass. Dir. Civ.*, 2014, III, 766, che afferma che «*la forza di espansione, valutativa e assiologica, del principio dello sviluppo sostenibile consente di estendere l'applicabilità dei criteri ambientali anche agli appalti privati*».

[82] Sulla tutela ambientale nei rapporti tra *cives*, con particolare riguardo agli strumenti negoziali: V. CARRIERO, *Sviluppo ecologico e strumenti negoziali di valorizzazione dei "beni culturali, paesaggistici e ambientali"*, in *Rivista quadrimestrale di diritto dell'ambiente*, 2020, I, 106 ss.. Sugli strumenti contrattuali per la tutela dei diritti umani e la protezione ambientale: L. VALLE, M.C. MARULLO, *Contract as an Instrument Achieving Sustainability and Corporate Social Responsibility Goals*, in *International Community Law Review*, 2022, Vol. 24, 100 ss.. Sui contratti ecologici tra diritto pubblico e diritto privato, cfr. C. IRTI, *Gli "appalti verdi" tra pubblico e privato,* in *Contratto e Impresa/Europa*, 2017, 183 ss., che mette in relazione la normativa di stampo pubblicistico in materia di appalti anche ai contratti verdi del diritto privato.

[83] In questo senso, si veda anche M. PENNASILICO, *Contratto e uso responsabile delle risorse naturali*, in *Rass. Dir. Civ.*, 2014, III, 764, secondo cui «*il mercato può rivelarsi un potente alleato della regolazione nel perseguimento delle finalità di tutela ambientale*».

[84] Sull'espressione contratto ecologico, cfr. S. PAGLIANTINI, *Sul c.d. contratto ecologico*, in *Nuova Giur. Civ.*, 2016, II, 20337 ss., secondo cui «*contratto ecologico, questo il succo del discorso, è un'espressione raffinata ma predicata di un valore soltanto descrittivo*». Si veda anche M. PENNASILICO, *Contratto e uso responsabile delle risorse naturali* cit., 768, per il quale «*il "contratto ecologico" è, dunque, applicazione privilegiata del paradigma intergenerazionale, che ispira la trasformazione dell'economia di mercato in "economia di mercato sociale ed ecologica"*». Quest'ultima definizione, fatta propria dall'A., è di P. HÄBERLE, *Potere costituente (teoria generale),*

più pervasivi di quanto avvenga nella contrattualistica pubblica, come nel caso delle operazioni di finanziamento alle società per azioni in relazione ai fattori ESG. Il contratto, in questo modo, diviene il luogo di realizzazione di interessi non soltanto suscettibili di valutazione economica, ma di interessi patrimoniali sostenibili [85] : l'inserimento di clausole sulla sostenibilità nella libera contrattazione tra privati implica valutazioni di carattere direttamente o indirettamente patrimoniale, ma in ogni caso meritevoli di tutela, in quanto aventi ad oggetto la sostenibilità[86].

Nei rapporti tra aziende e utenti finali, poi, si avverte un progressivo avvicinamento dei principi propri della tutela consumeristica agli obiettivi generali dell'economia circolare. Nello specifico, appare opportuno un adeguamento alla logica di sostenibilità del mercato, il quale implica anche una concreta ed efficace applicazione del diritto all'informazione dell'utente, in grado di orientare le sue scelte in modo sostenibile. In tale ottica, spetterà all'utente di un prodotto o servizio di IA privilegiare scelte coerenti con un mercato sostenibile. In questo contesto, la trasparenza nell'etichettatura, la configurazione di un nuovo ambito di illiceità contrattuale connotato dalla violazione della sostenibilità, costituzionalmente protetta, così come il rafforzamento delle garanzie di durata dei beni di consumo sono strumenti di diritto privato che mirano ad una economia circolare[87].

Pertanto, il concetto di sostenibilità a tutto tondo, e quindi non solo di sostenibilità ambientale, ma anche sociale ed economica, si avverte sempre più

---

in *Enc. Giur.*, Agg., IX, Roma, 2000, 40. Ancora dello stesso A., più di recente, si vedano M. PENNASILICO, *Il "contratto ecologico" tra Italia e Cina: verso un nuovo paradigma giuridico"*, in *Annuario di diritto comparato e di studi legislativi*, 2021, 169 - 205; ID.: *"Proprietà ambientale" e "contratto ecologico: un altro modo di soddisfare i bisogni*, in *Rass. Dir. Civ.*, 2018, IV, 1261 - 1290; ID.: *Contratto ecologico e conformazione dell'autonomia negoziale*, in *Quarterly Journal of Environmental Law*, 2017, I, 4 ss..

[85] M. PENNASILICO, *Contratto e uso responsabile delle risorse naturali,* cit., 768, evidenzia come oggi il contratto sia fonte non semplicemente di rapporti giuridici patrimoniali, bensì di rapporti giuridici patrimoniali sostenibili. L'Autore ritiene aprirsi così una nuova stagione del contratto: una stagione "verde" fondata sull'analisi "ecologica" del diritto contrattuale, che consente di cogliere che la nozione stessa di contratto *ex* art. 1321 c.c. è ormai insufficiente se non integrata con i princípi di solidarietà e di sostenibilità nell'uso responsabile delle risorse naturali. Cfr. altresì S. PERSIA, *Proprietà e contratto nel paradigma del diritto civile "sostenibile"*, in *Rivista quadrimestrale di diritto dell'ambiente*, 2018, I, 11, secondo cui «*Il contratto, in questa "circolarità" tra ambiente e mercato, si fa portatore di interessi non solo patrimoniali ma altresì non patrimoniali, compatibili con il pieno sviluppo della persona umana, e si accredita come contratto "ecologico", fonte non semplicemente di rapporti giuridici patrimoniali, ma di rapporti giuridici patrimoniali sostenibili*».

[86] M. PENNASILICO, *Contratto e uso responsabile delle risorse naturali*, cit., 765, che afferma che «*la centralità che le esigenze ambientali, sottese alle ipotesi di obbligatorietà degli appalti verdi, hanno ormai guadagnato nell'ordinamento italo-europeo, imponendo una conformazione "ecologica" dell'autonomia negoziale, induce a riconoscere che la meritevolezza dei "contratti verdi" è* in re ipsa *nella liceità della causa: in effetti, il giudizio di meritevolezza appare pleonastico se riferito a contratti diretti a soddisfare interessi ambientali leciti, che "colorano" la causa concreta e sono in armonia con il «pieno sviluppo della persona umana» (art. 3, comma 2, Cost.)*». Per un'attenta riflessione sulla meritevolezza di tutela degli interessi contrattuali in relazione alla tutela ambientale si veda P. PERLINGIERI, *Persona, ambiente e sviluppo*, in *Contratto e ambiente. L'analisi "ecologica" del diritto contrattuale* (a cura di PENNASILICO M.), Napoli, ESI 2016, 321 ss., secondo il quale anche se il contratto contiene clausole sulla tutela ambientale non è comunque meritevole di tutela qualora si ponga di fatto in contrasto con valori quali la salute dell'uomo e la sua integrità psico-fisica.

[87] In tal senso M.A. CIOCIA, *Circolarità economica e trasparenza del prodotto*, in *EJPLT*, 2022, I, 57-72, DOI: https://doi.org/10.57230/EJPLT221MAC. L'approccio antropocentrico per la sostenibilità è particolarmente importante in relazione ai prodotti intelligenti, in quanto il consumatore in ambiente digitale si trova in una posizione di vulnerabilità strutturale: L. GATT, I.A: CAGGIANO, *Consumers and Digital Environments as a Structural Vulnerability Relationship*, in *EJPLT*, 2022, II, 8 - 16.

forte anche nelle contrattazioni tra privati [88]. Partendo dalla sostenibilità ambientale e poi estendendola alle sue diverse declinazioni, devono essere individuati criteri *ad hoc*, per implementare la stessa nelle produzioni aziendali di IA ovvero caratterizzate da IA e, contemporaneamente, vanno previsti modelli contrattuali compatibili con gli obiettivi di sostenibilità fissati dalle politiche pubbliche eurounitarie [89] e internazionali, oltre che nazionali, incentrati, nel caso di specie su clausole di sostenibilità delle attività d'impresa, soprattutto in relazione alle applicazioni di IA.

In particolare, nella regolamentazione contrattuale dei rapporti che hanno ad oggetto la fornitura di prodotti di IA, è opportuno sviluppare strumenti di natura privatistica, i quali prevedano un diritto di prelazione nei rapporti contrattuali in favore delle aziende che rispettino elevati standard di sostenibilità. La previsione di tali criteri di sostenibilità nella contrattualistica privata appare oltremodo significativa nel settore dell'IA in quanto, ad esempio, essa risente particolarmente degli obiettivi di transizione ecologica ed elettrificazione fissati a livello di Unione europea e che da tali obiettivi deve cercare di trarre nuove opportunità di sviluppo. Ed è così che diviene cruciale per le imprese coinvolte nella filiera dei prodotti intelligenti prevedere nei contratti aziendali clausole atte a garantire lo sviluppo di un'IA sostenibile.

Nello specifico, il diritto di essere preferiti potrebbe derivare dalla sussistenza di determinati requisiti di sostenibilità – conformi ai fattori ESG – e costituire una clausola di prelazione volontaria, soggetta alla libera autonomia delle parti che intendono agire responsabilmente e, auspicabilmente, in un prossimo futuro, rappresentare una prelazione legale.

4. Sviluppo sostenibile dell'IA nella prospettiva della tutela dei *green rights*.

Secondo quanto analizzato nel presente lavoro, nella società contemporanea i diritti aumentano o, comunque, evolvono come conseguenza dei nuovi possibili rischi, per i quali occorre trovare una tutela anche giuridica.

Ciò vale ad esempio nel caso dello sviluppo del settore industriale con particolare riguardo alle tecnologie di IA, le quali comportano il sorgere di potenziali vantaggi, ma anche di possibili rischi per l'individuo e per il pianeta.

Tuttavia, non sembra necessaria la moltiplicazione di norme settoriali in relazione al mutamento di determinate fattispecie giuridiche, ora particolarmente soggette allo sviluppo tecnologico. L'età in cui viviamo è

[88] Sulle clausole di sostenibilità si veda S. LANDINI, *Clausole di sostenibilità nei contratti tra privati. Problemi e riflessioni*, in *Diritto pubblico*, 2015, II, 611 ss..

[89] Per un approfondimento sulle politiche pubbliche dell'UE aventi ad oggetto le valutazioni di impatto sulla sostenibilità - VIS (*Sustainability Impact Assessment* – SIA) nelle contrattazioni pubbliche commerciali con paesi extra-UE, si rinvia alla pagina ufficiale della Commissione europea: https://policy.trade.ec.europa.eu/analysis-and-assessment/sustainability-impact-assessments_en. La valutazione d'impatto sulla sostenibilità (VIS) è uno strumento che consente di effettuare un'analisi approfondita dei potenziali impatti economici e sociali sui diritti umani e sull'ambiente dei negoziati commerciali in corso. Essa è stata sviluppata dalla Direzione generale del Commercio della Commissione europea (DG Trade) nel 1999 per i negoziati della *World Trade Organization Doha Development Agenda* (DDA).

immotivatamente caratterizzata dal proliferare di norme che si susseguono l'un l'altra, anche in modo confuso, minando le basi della certezza del diritto[90].

Allo stesso modo, non occorre estendere oltremodo le categorie giuridiche esistenti nella convinzione di poter così garantire una maggiore tutela dell'individuo, come nel caso sopra analizzato dei diritti della natura. Infatti, categorie giuridiche ben precise già esistono: il bene giuridico "natura" e la tutela della stessa quale oggetto dei diritti dell'individuo.

Ciò che sembra in parte mancare, invece, sono leggi efficaci[91], anche nell'ottica di una fortificazione della tutela *ex ante*, partendo dalla reinterpretazione di quei diritti fondamentali dell'uomo più strettamente connessi al concetto di sostenibilità, per rispondere alle esigenze delle generazioni presenti e future (primi tra tutti i *green rights*).

Il principio di sostenibilità in chiave antropocentrica, con riferimento al settore dell'IA, può essere messo in pratica con una regolamentazione multilivello (almeno europea, se non internazionale)[92], composta da diverse tipologie di atti normativi: non solo di *hard law*, ma anche di *soft law* (dalle linee guida ai codici di condotta), oltre che da precise norme tecniche (es. standard) – applicabili anche tramite il rinvio operato da norme giuridiche vincolanti – e tecno-regolamentazioni, in un'ottica di ibridazione dei saperi[93].

Al centro della regolamentazione, per il settore dell'industria 4.0. va collocata anche la RDI la quale, se ben implementata può effettivamente contribuire allo sviluppo di un'IA sostenibile tanto "per" la produzione che "nella" produzione. Una RDI intesa in senso ampio, estesa agli obiettivi di sostenibilità a tutto tondo, deve includere *policy* aziendali incentrate sui fattori

---

[90] F. Capra e U. Mattei, *Ecologia del diritto. Scienza, politica, beni comuni,* Sansepolcro, 2017, 12 ss., evidenziano la necessità di trasformare il diritto per creare un «ordine giuridico ecologico» e in particolare di «dissociare il diritto dal potere e dalla violenza; rendere la comunità sovrana; rendere la proprietà generativa». P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, 3ª ed., Napoli, 2006, 16, il quale definisce la legislazione come «affannosa» e «alluvionale» criticandola, inoltre, per essere sempre più frequentemente caratterizzata da tecniche legislative che non mirano ad una visione globale della fattispecie giuridica, che tenga conto anche del quadro costituzionale e sovranazionale. In tal senso anche C. Caccavale, *Per un diritto sostenibile*, in *Crisi della legge e produzione privata del diritto*, a cura di G. Conte, M. Palazzo, 2018, II, 241 ss.. che espone chiaramente, criticandola, l'eccessiva produzione di norme giuridiche. Sulla mancanza di una effettiva cogenza delle norme giuridiche si veda M. Orlandi, *Norme deboli*, in *Liber amicorum. Pietro Rescigno. In occasione del novantesimo compleanno*, II, Napoli, 2018, 1451 ss.; Id., *Diritto mite*, in *Il problema delle leggi imperfette, Etica della partecipazione all'attività legislativa in democrazia*, a cura di L. Eusebi, Brescia, 2017, 107 ss..

[91] Per un approfondimento del concetto di efficacia si rinvia a I.A. Caggiano, *A Quest for Efficacy in Data Protection: a Legal and Behavioural Analysis*, in *Universidad de Barcelona Jean Monnet Chair Working Papers 10/2017*, 6 ss., in cui l'Autrice analizza l'efficacia degli strumenti normativi con particolare riguardo al reg. 2016/679/UE (c.d. GDPR) sulla protezione dei dati personali.

[92] Infatti, la regolamentazione dovrebbe essere fornita a livello internazionale, europeo e nazionale. Il livello nazionale dovrebbe essere il risultato del confronto con altri ordinamenti più virtuosi, nonché del recepimento della normativa sovranazionale. Come sostenuto da T.E. Frosini, *Il metodo*, in *Diritto pubblico comparato. Le democrazie stabilizzate* (a cura di T.E. Frosini), Bologna, 2019, 13 - 14, il diritto comparato serve a contribuire all'evoluzione e al progresso di un ordinamento giuridico, attraverso le esperienze giuridiche che si sono prodotte in terra straniera.

[93] Sulla metodologia dell'ibridazione dei saperi, cfr. L. Gatt, *The reasons for choosing a hybrid method of investigation and the relationship with technology*, in Aa.Vv., *Privacy and Consent. A Legal and UX&HMI Approach for data protection*, a cura di L. Gatt., I.A. Caggiano, R. Montanari, Suor Orsola Benincasa University, Napoli 2021, 12 -13.

ESG, nonché contratti d'impresa caratterizzati da clausole di sostenibilità dell'IA sia tra professionisti (B2B) che con i consumatori (B2C)[94].

Ciononostante, si avverte una resistenza delle aziende nell'investire in una solida cultura di responsabilità digitale d'impresa, derivante tanto dai costi associati a tali iniziative, quanto dalla mancanza di consapevolezza o di competenze tecniche necessarie, oltre alla difficoltà di dover conciliare obiettivi di *business* con l'implementazione di sistemi di gestione adeguati. Infatti, non sempre gli obiettivi aziendali di *business* vanno di pari passo con i principi di sostenibilità, anzi, nella pratica ciò accade raramente.

L'uso delle tecnologie di IA migliora e ottimizza le *performance*: per esempio, le promozioni mirate e la vendita incrociata sono efficaci nell'aumentare le vendite, l'*engagement* e la *retention* degli utenti. Esse, inoltre, aiutano a migliorare l'esperienza dell'utente (*user experience* - UX) grazie a personalizzazione e sistemi di raccomandazioni basati appunto sui dati raccolti. Le automazioni e i sistemi di IA, poi, riducono i costi e l'inquinamento ambientale, ottimizzando e automatizzando i processi.

Per gestire eticamente i processi di produzione, però, sono necessarie norme efficaci (come potrebbero esserlo quelle che disciplinino il diritto di prelazione e le clausole di sostenibilità dell'IA, l'etichettatura dei prodotti, l'illiceità contrattuale per violazione della sostenibilità [95]) e la formazione di *team* integrati che conoscano ed attuino pratiche conformi ed efficaci a tutti i livelli, che non solo siano allineati alla regolamentazione normativa ma che creino e adottino delle procedure standardizzate. Questo non solo riduce i rischi dell'impatto negativo dell'IA, ma rafforza anche la fiducia degli *stakeholder*, la fiducia degli utenti e consolida la reputazione aziendale.

Pertanto, lo sviluppo di un'IA sostenibile richiede un approccio strategico, integrato e transdisciplinare[96]. È essenziale che venga implementata anche tra privati, e quindi nel diritto privato, una gestione responsabile di tutto il ciclo produttivo dell'IA, per garantire un ecosistema dell'IA sicuro e affidabile a tutti i livelli e per tutte le parti coinvolte.

In particolare, occorre sviluppare anche nel diritto privato un concetto di sostenibilità a tutto tondo[97], non solo ambientale, quindi, ma anche sociale ed economica, prendendo ad esempio i fattori ESG ed estendendo il loro ambito di applicazione, nonché mettendo in atto un'analisi dei processi, delle aree e delle funzioni dei differenti rapporti tra privati (B2B e B2C). L'approccio deve essere proporzionale alle dimensioni dell'affare, al settore di riferimento, al

---

[94] I contratti del consumatore rientrano nel novero dei contratti d'impresa quali contratti tra l'impresa e il consumatore (definiti anche contratti unilaterali d'impresa). Si veda in tal senso V. BUONOCORE, *Contratti del consumatore e contratti di impresa*, in *Riv. dir. civ.*, 1995, I, 41, il quale sostiene che «piuttosto che un polo antitetico alla contrattazione d'impresa, i contratti dei consumatori costituiscono un segmento di fondamentale importanza per la stessa».

[95] Per un approfondimento su illiceità del contratto e sostenibilità si rinvia a R. FADDA, *La sostenibilità tra disciplina del contratto e tutela del consumatore*, Napoli, 2024, 40 - 45.

[96] Mentre la multidisciplinarietà mette in campo la collaborazione tra discipline verso il raggiungimento di obiettivi prestabiliti, la transdisciplinarietà comporta la collaborazione tra discipline già dalla fase di identificazione degli obiettivi. Cfr. Position Paper dell'Agenzia per la Promozione della Ricerca Europea, *Verso FP10*, giugno 2024, 7 e 8.

[97] In tal senso E. CATERINI, *Sustainability and Civil Law*, in *The Italian Law Journal*, Vol. 4, II, 2018, ritiene che «*Sustainability has become the social analysis of law*» e sottolinea la necessità di un mercato sostenibile a livello europeo, 289 - 297.

mercato di competenza e, soprattutto, agli obiettivi che si intendono perseguire.

Il valore del mercato non è più solo direttamente economico-produttivo, ma è la promozione di un valore volto allo sviluppo sostenibile, a beneficio di un nuovo modello di economia responsabile che garantisca un'IA sostenibile per la tutela dei diritti dell'uomo, primi tra tutti i *green rights*.

De Mari Casareto dal Verme T, 'Civil liability regimes for AI-related torts within the Italian legal system' (2024) 2 EJPLT, 172 – 190.
DOI: https://doi.org/10.57230/EJPLT242TDMCDV

EJPLT
ISSN 2704-8012



Civil liability regimes for AI-related torts within the Italian legal system

I criteri di imputazione della responsabilità civile per i danni cagionati dall'IA nell'ordinamento giuridico italiano

TOMMASO DE MARI CASARETO DAL VERME
Research Fellow in Private Law
University of Trento

Abstract

The paper addresses the issue of ascribing civil liability for torts committed by 'intelligent software agents', i.e., tangible or intangible product equipped with Artificial Intelligence (AI) in the 'modern' sense of the term. As the latest proposals and forthcoming EU legislation do not affect the core of liability regimes existing at national level, it is necessary to investigate the features and operational rules of the liability regimes destined to play a central role when it comes to AI-related torts. In the Italian legal system, the outcome of the analysis shows that the so-called 'responsibility gap' generated by AI can be filled by providing for appropriate interpretative adjustments to the 'traditional' tort law rules in the light of the peculiarities of modern AI. In this respect, Italian tort law shows to be flexible enough to also cover damages caused by smart products, still reaffirming the need to strike a balance between individuals' rights protection and incentivizing technological innovation.

© The author(s) 2024, 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 contributo affronta il tema dell'imputazione della responsabilità civile per gli illeciti commessi da agenti artificiali intelligenti, ossia da qualsiasi prodotto, materiale o immateriale, dotato di Intelligenza Artificiale (IA) in senso "moderno". Poiché le ultime proposte dell'Unione Europea (UE) sul tema non incidono sul nucleo dei criteri di imputazione della responsabilità esistenti a livello nazionale, è necessario indagare le caratteristiche e le regole operative delle regole di responsabilità destinate a svolgere un ruolo centrale quando si tratta di illeciti cagionati dall'IA. Nell'ordinamento italiano, l'esito dell'analisi mostra che il cosiddetto "responsibility gap" generato dall'IA può essere colmato attraverso un'attenta opera di interpretazione evolutiva delle norme "tradizionali" alla luce delle peculiarità dell'IA moderna. In questo senso, il diritto italiano della responsabilità civile si dimostra sufficientemente elastico da regolare anche le fattispecie di danni causati da smart products, pur riaffermando la necessità di individuare il giusto equilibrio tra tutela dei diritti e progresso tecnologico.

Keywords: Artificial Intelligence; civil liability; defective AI systems; custody over AI systems

Summary: 1. Introduction. – 2. The 'responsibility gap' doctrine. – 3. AI and tort: the ground for a horizontal approach. The Intelligent Software Agent. – 4. The liability regimes for the Intelligent Software Agent. – 5. The liability of the manufacturer. – 5.1. The proof of defectiveness: the 'model software agent'. – 5.2. The defenses. – 6. The liability of the user: the 'custody' over the software agent. – 7. Conclusions.

1. Introduction.

Artificial Intelligence (AI) represents one of the leading actors of the so-called Fourth Industrial Revolution ('Industry 4.0').[1] Despite the birth of AI as a scientific discipline dating back to the 1950s,[2] today's society is in the heat of a new 'summer' of its development, where the advancements in the research allow AI to get novel and unprecedented features. In fact, although identifying a clear definition of Artificial Intelligence is a major challenge even within the scientific community, it is possible to understand the 'modern approach' to AI research in opposition to what is to be intended as traditional AI. Russel and

[1] The origin of the term can be traced back to its first use in 2011 when, during the Hannover Messe, Henning Kagermann, Wolf-Dieter Lukas and Wolfgang Wahlster - business, technology and industry leaders as well as advisors to the German government - released their paper entitled '*Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution*'. Industri 4.0 is mainly characterized by a fusion of physical and digital spheres which gives rise to complex cyber-physical systems. For deeper insights, see K Schwab, *The Fourth Industrial Revolution* (1st edn, Portfolio Penguin, 2017); A Ustundag, E Cevikan, *Industry 4.0: Managing the Digital Transformation* (Springer, 2018) 4-5.

[2] The father of AI is often identified in Alan Turing, who in the 1950s studied the theoretical possibility of answer the question 'can machines think?' in his famous article AM Turing, 'Computing Machinery and Intelligence' (1950) 49 Mind, 433. Subsequently, the official birth of Artificial Intelligence as a real scientific discipline is traced back to 1956, the year of the *Dartmouth Summer Research Project on Artificial Intelligence*, where some scientist proposed 'that a 2 month, 10 men study of artificial intelligence be carried out during the summer of 1956 at Dartmouth College in Hanover, New Hampshire' (J McCarthy, M Minsky, N Rochester, C Shannon, 'A Proposal for the Dartmouth Summer Research Proect on Artificial Intelligence', 31 August 1955, available at: http://www.aaai.org./ojs/index.php/aimagazine/article/view/1904).

Norvig start from a central question: 'why would we want a machine to learn?', and they provide for two main reasons: 1) the designers cannot anticipate all possible situations that the agent might find itself in; 2) sometimes human programmers have no idea how to program a solution themselves.[3]

It is possible to affirm that learning techniques represent the main feature of 'modern AI', which is capable of acting autonomously, learning from its own experience, evolving and improving its performance over time. This is possible today thanks to the implementation of machine learning (ML) and deep learning (DL) techniques combined with the huge development of computers' power and the global diffusion of Internet. In fact, the primary characteristic of modern AI lies in its ability to draw inferences and identify patterns beyond human capabilities, thanks to ML and DL algorithms that enable advanced forms of learning directly from raw data and self-generated experiences, all without relying on human expertise.[4] This marks the transition from mere automation to autonomy.[5]

However, as is often the case, the main drivers of technological innovation come with as many risks to which the law must turn its attention since they are capable of generating possible protection gaps that legislators, and the EU legislator in particular, are called upon to address.

First of all, unlike previous industrial revolutions, characterized by more or less sector-specific 'symbolic technologies', AI struggles to be classified as a proper 'technology', since by its very nature it constitutes a cross-cutting approach capable of potentially affecting any type of product to be released on the market and assuming as many facets as its potential domains of application. This is why defining AI has proved to be among the most challenging tasks for the EU in the past years. Eventually, the supranational legislator had to opt for a horizontal approach to AI regulation, resulting in the adoption of the Artificial Intelligence Act ('AI Act')[6] which sets out *ex-ante* safety rules for the release of 'high-risk' AI systems into the market, irrespective of whether they are embedded in other final products or they are placed on the market independently.[7] Within the new Regulation the definition of 'AI system' is quite broad, encompassing every «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,

[3] S Russel, P Norvig, *Artificial Intelligence. A modern Approach* (4th edn, Pearson Education Limited, 2022) 669.
[4] Machine learning (ML) focuses on the development of algorithms and models that enable computers to learn from data and make predictions or decisions without explicit programming. The core idea is to allow machines to improve their performance on a specific task over time by learning from experience. Deep Learning does the same but employs many layers of neural networks where the inner layers are not designed by human engineers but are learned by the system autonomously through data collection and processing, employing general learning methods. For deeper insights, see E Alpaydin, *Introduction to Machine Learning* (3rd edn, The MIT Press, 2014); I Goodfellow, Y Bengio, A Courville, *Deep Learning* (The MIT Press, 2016).
[5] D Powell, 'Autonomous Systems as Legal Agents: Directly by the Recognition of Personhood or Indirectly by the Alchemy of Algorithmic Entities' (2020) 18(1) Duke Law Technol. Rev. 310, pointing out that the distinguishing element between autonomy and mere automation is the ability to learn and adapt to unforeseen circumstances.
[6] 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, AI Act).
[7] See Article 6, par. 1 AI Act.

infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments».[8]

Second, the complexity that characterizes modern AI systems' learning capacities, on the one hand, makes it difficult (even for their creators) to understand how and why a specific output has been generated – giving rise to the 'black box' phenomenon –[9], and such challenge is even exacerbated by the information asymmetries existent between consumers and professionals who monopolize the technology and the information related to it, especially in the digital environment where consumers face a form of new and 'structural' vulnerability.[10] On the other hand, gives the algorithmic decisions an inevitable degree of unpredictability and ungovernability. In this respect, the AI Act is concerned with ensuring the highest possible level of safety for high-risk AI systems by setting preventive rules on transparency and human oversight. Nevertheless, an *ex-ante* perspective is not sufficient *per se* to prevent every technology-related risk. Therefore, there is a percentage of risk that cannot be eliminated by a preventive approach; hence a problem of *ex-post* liability arises in the case of damage caused by an AI system although regularly placed on the market.[11]

2. The 'responsibility gap' doctrine.

The problem of ascribing civil liability for damages caused by AI traces back to the so-called 'responsibility gap doctrine',[12] which highlighted the possible gaps in protection caused by the aforementioned features of modern AI systems and their possible conflict with the traditional tort rules existing mainly at national level.[13] The responsibility gap doctrine in the field of AI was

[8] Article 3(1) AI Act.

[9] On the topic, F Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015); T Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box', in T Wischmeyer, T Rademacher (eds.), *Regulating Artificial Intelligence* (Springer, 2020) 75 ff.

[10] See L Gatt, IA Caggiano, 'Consumers and Digital Environments as a Structural Vulnerability Relationship' (2022) 2 EJPLT 12, who highlight that 'the crucial point lies in the determination of a concept of vulnerability that is not linked to specific physical or psychological disabilities but is identified in the relationship between the physical person and the technological environment in which he/she operates', giving rise to an 'ontological vulnerability of human beings – in general – with respect to digital technology structures. See also L Gatt, 'Legal anthropocentrism between nature and technology: the new vulnerability of human beings' (2022) 1 EJPLT 15 ff.; AA Mollo, 'La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici' (2021) 1 EPJLT 201 ff.

[11] In the EU legal system safety rules are generally set out by preventive regulations or directives informed by the so-called 'New Legislative Framework', intended to pose minimum ex-ante safety requirements that products must comply with in order to be regularly placed on the EU market. Nevertheless, such rules can cover just a limited percentage of risks, while tort law deals with regulating also additional risks which are not entirely preventable. On these topics, see N Scannicchio, 'Il diritto privato europeo nel sistema delle fonti', in N Lipari (ed), *Trattato di diritto privato europeo*, vol I (2nd edn, Cedam 2003), 21; E Bellisario, 'Il danno da prodotto conforme tra regole preventive e regole risarcitorie' (2016) 3 Eur. dir. priv. 842; R Montinaro, 'Difetto del prodotto, norme tecniche ed informazione sui rischi di danno alla salute' (2019) 1 Resp. civ. prev. 289.

[12] A Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata' (2004) 6 Eth. Inf. Tech. 175.

[13] For a general reconstruction of the debate in Italy, see C Scognamiglio, 'Responsabilità civile ed intelligenza artificiale: quali soluzioni per quali problemi?' (2023) 4 Resp. civ. prev. 1082; G Finocchiaro, 'Intelligenza artificiale, diritto e responsabilità', in P Perlingieri, S Giova, I Prisco (eds), *Rapporti civilistici e*

originally framed in the philosophical debate to indicate the concern that machine learning was likely to make it more difficult, or even impossible, to attribute 'moral' blame to individuals for the consequences of unpleasant events related to its use.[14] Following, part of tort law scholars have emphasized how the renewed degree of uncertainty and risk generated by the advent of intelligent technologies has led to the question of whether existing legal norms are adequate to regulate the phenomenon or whether there is need for their general revision.[15]

Indeed, the capacity of AI of evolving and changing autonomously – as well as the inaccessibility and uncontrollability of the information stored in it and the unpredictability of its decisions – can cause a loss of control over the system by both its programmer and user, a circumstance that could make it unjustified to ascribe responsibility to such parties. Therefore, the existence of a liability gap in cases of damages caused by autonomous and unpredictable AI systems was pointed out since control and predictability are supposed to be necessary requirements for the attribution of liability to a human being, regardless of the specific liability basis of reference.[16]

The mentioned responsibility gap would result in making it difficult or even impossible for the injured parties to get effective access to justice, due to the complexity of complying with the burden of proof lying on them according to their own national legislation when it comes to AI-related tort.[17] Such complexity exists both when an action is brought against the manufacturer of the AI system and against its user. In the former case, the applicability of the Product Liability Directive (PLD) –[18] as transposed in each Member State's legislation – comes into play, which holds the manufacturer liable for damages caused by its defective product and requires the injured party to prove the defect, the damage, and the causal link between defect and damage. In the latter case, user liability is basically grounded on fault, and the injured person is required to prove the causal link between the damage and the fault of the liable party. Other times, as in Italian law, there are strict liability rules suitable to help the injured party in fulfilling their burden of proof.

---

intelligenze artificiali: attività e responsabilità. Atti del 15° Convegno Nazionale 14-15-16 maggio 2020 (ESI, 2020), 27; F Caroccia, 'Ancora su responsabilità civile e uso delle intelligenze artificiali' (2022) 2 Contr. impr. 408; C Leanza, 'Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio' (2021) 3 Resp. civ. prev. 1020; A Bertolini, 'Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules' (2013) 5(2) L. Innov. Tech. 233; G Sartor, 'Gli agenti software e la disciplina giuridica degli strumenti cognitivi' (2003) 1 Dir. inf. 55.

[14] F Santoni De Sio, G Mecacci, 'Four Responsibility Gaps with Artificial Intelligence: Why they Matter and How to Address Them' (2021) 34 Phil. Tech. 1057.

[15] The initial debate was divided between a *de lege lata* approach, which emphasized the sufficiency of existing legal norms to fill a gap that was therefore only be apparent, and a *de lege ferenda* approach, which looked, instead, favorably to the introduction of *ad hoc* legal rules for AI, emphasizing its characteristics of absolute novelty. For an overview, see U Ruffolo, 'Intelligenza artificiale, machine learning e responsabilità da algoritmo' (2019) 7 Giur. it. 1689; G Taddei Elmi, F Romano, 'Il robot tra ius condendum e ius conditum' (2016) 1 Inf. dir. 115; A Santosuosso, C Boscarato, F Caroleo, 'Robot e diritto: una prima ricognizione' (2012) 7-8 Nuova giur. civ. comm. 494.

[16] PM Asaro, 'The Liability Problem for Autonomous Artificial Agents' (2016) AAAI Spring Symposium Series 191; Id., 'Robots and Responsibility from a Legal Perspective' (2007) Proceedings of the IEEE.

[17] On the topic, see M Faccioli, 'La responsabilità civile per danni cagionati da sistemi di Intelligenza Artificiale nel prisma dell'onere della prova' (2024) 3 Resp. civ. prev. 950.

[18] Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC).

The EU has been addressing the issues related to the AI responsibility gap since the adoption of the Resolution of 16 February 2017 on civil law rules on robotics, [19] where the European Parliament reached the conclusion that traditional tort rules were inadequate for facing the features of modern AI and that new ones were necessary. This approach also emerges in the Resolution of 20 October 2020,[20] where the European Parliament proposed a special liability regime allocating various degrees of responsibility to AI 'operators' based on the level of risk posed by the AI system. Thereafter, the European legislator took a more nuanced stance by adopting two directive proposals on 28 September 2022 aimed at harmonizing some liability rules in order to alleviate the burden of proof on injured parties. The first one, known as 'AI Liability Directive' ('AILD'), [21] addresses non-contractual fault-based liability claims brought before national courts in cases where damage originates from an AI. The second one is a new Product Liability Directive proposal[22] which aims at revising and replacing the current PLD in light of the latest developments in modern digital technologies, including AI. The new PLD has been officially adopted in October 2024[23].

Although both the mentioned proposals outline specific liability rules on the burden of proof, they do not affect the applicability of the ordinary liability regimes existing at national level. Moreover, the proof-alleviation mechanisms provided therein could even not be activated and the presumptions can be rebutted.[24] In particular, in the new PLD the proof of defectiveness remains unchanged in its substance, still grounding it on the so-called 'consumer expectation test'.[25] This choice confirms that large part of the subject will be left to the liability regimes as in force and interpreted by the courts at national level. Accordingly, the relationship between AI and civil liability must start from the analysis of the liability regimes existing at national level to test whether they are consistent with the features of modern AI.

[19] European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C 252/25).
[20] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).
[21] COM(2022) 496 final 2022/0303 (COD) Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).
[22] COM(2022) 495 final 2022/0302 (COD) Proposal for a Directive of the European Parliament and of the Council on liability for defective products.
[23] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.
[24] The weakness of the proposals was pointed out in the sense that, on the one hand, the presumptions provided for therein could easily be rebutted by the defendant and, on the other hand, the disclosure mechanism would not necessarily help the injured party, who might be overwhelmed by an information overload, where complex technical information could complicate the burden of proof. For deeper insights, see P Hacker, 'The European AI liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future' (2023) 51 Com. L. Sec. Rev. 10; 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 Resp. civ. prev. 656, 670.
[25] G Veldt, 'The New Product Liability Proposal – Fit for the Digital Age or in Need of Shaping Up?' (2023) 1 EuCML 26. See also J-S Borghetti, 'Taking EU Product Liability Law Seriously: How Can the Product Liability Directive Effectively Contribute to Consumer Protection?' (2023) 1 Fr. Journ. Pub. Pol. 33, 35 available at: https://ssrn.com/abstract=4502351, according to which maintaining the same definition of defective product is the only possible way to regulate the wide variety of products equipped with AI.

3. AI and tort: the ground for a horizontal approach. The Intelligent Software Agent.

The perspective adopted for the investigation of the problems described is horizontal and cross-cutting. Significantly, the object of analysis is AI as such, regardless, that is, of its specific technological application fields. This methodological choice is justified by the very nature of the phenomenon, which manifests itself with a transversal or 'ubiquitous'[26] dynamic with respect to specific application sectors and influences what can be considered reasonable and predictable beyond the single technological contexts of reference.[27] Therefore, the analysis must transcend the boundless variety of AI applications and search for common denominators to be taken as a reference in order to elaborate categories that are as unifying as possible and likely to be applied to every sector manned by AI.[28]

To do so, it is necessary to identify the transversal aspects of AI relevant from a legal point of view as potentially challenging the applicability of ordinary tort rules. In the interests of simplification in the legal analysis, we propose a unifying and abstract category encompassing all the relevant features of AI. In this respect, the category of 'Intelligent Software Agent' is proposed here, functional to encapsulate any type of smart product, whether physical or virtual, regardless of the specific context in which it operates.[29] Such an agent is capable of collecting data through sensors, processing raw data, planning and performing actions through the knowledge and information gained, evolving, learning and improving its performance when generating its outputs. The combination of these characteristics gives the software agent a degree of unpredictability and opacity, in that it allows algorithms to evolve from their initial programming in ways that are not always predictable and understandable by those who created them or those who use them.

Thus, although the agent undergoes an intensive training phase prior to its deployment, the rules under which it makes decisions are not entirely fixed at the production stage but may change in the course of its operation. In fact, if the agent relied solely on the knowledge imparted by its programmer rather than on its own perception, the character of autonomy would be lacking.[30]

---

[26] R Leoncini, M Macaluso, 'Gli effetti economici dell'intelligenza artificiale', in VV Cuocci, FP Lops, C Motti (eds), *La responsabilità civile nell'era digitale* (Cacucci, 2022), 90.

[27] See W Barfield, U Pagallo, *Advanced Introduction to Law and Artificial Intelligence* (Edward Elgar, 2020), 95, who highlight that the regulation of AI liability is particularly complex due to the fact that some sectors where AI is applied already have specific regulations in place. It is important to consider these existing regulatory frameworks that govern areas such as autonomous vehicles, drones, healthcare, financial services, and data protection. However, AI also influences what is considered reasonable and foreseeable beyond these individual sectors. Each example presents unique challenges in civil liability, but it is essential to first address the cross-cutting issues that affect all areas of AI application before focusing on the specific complexities of each sector.

[28] A Amidei, 'Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione europea' (2019) 7 Giur. it. 1718.

[29] For a more in-depth study, please refer to T De Mari Casareto dal Verme, *Intelligenza Artificiale e responsabilità civile. Uno studio sui criteri di imputazione* (Editoriale Scientifica, 2024), 113.

[30] Many proposals have been made for the definition of 'autonomy' with regard to computer systems. There are those who identify autonomy solely with the absence of human intervention in the functioning of the system and those who instead emphasizes the ability to evolve and modify one's own initial set of knowledge over time; others go so far as to define autonomy as the tension of the system towards a result that corresponds to its internal needs and representations. When it comes to civil liability, only software

These traits identify autonomy in decision-making and the ability to evolve as the main novelties compared to the past, potentially capable of challenging the validity of traditional tort law rules.[31]

In the view of the mentioned horizontal perspective, the liability regimes to be explored must be equally transversal and, accordingly, not sector-specific, since sector-specific liability regimes would not allow a unitary analysis to be conducted due to the dishomogeneity of the liability-generating factors contemplated in such cases.[32] This does not mean neglecting the importance of considering the specific interests underlying the various application areas of AI in each case, but before assuming a 'vertical' approach we deem necessary to investigate the common, horizontal profiles.[33]

4. The liability regimes for the Intelligent Software Agent.

First of all, it must be clarified that the notion of 'agent' employed here is not to be intended in a strict sense, but in a functional way. In fact, software agents must not be considered as proper agents – i.e., as conscious, self-aware entities – but as products, albeit highly sophisticated and capable of evolving. As regards tort law, all previous proposals that have attempted to give the software agent a nature other than product have been rejected by scholarship and institutions both for technical and legal reasons.

On the one hand, some scholars (and, at the beginning, the European Parliament as well)[34] have suggested to hold the AI system directly liable for damages, by creating an *ad hoc* legal personhood[35] on the model of how it happens already for corporations, which are entitled to rights and duties recognized by the legal system, although they are not natural persons.[36]

---

agents capable of learning and evolving over time are considered properly autonomous (and not merely automated). On the topic, see G Sartor, A Omicini, 'The Autonomy of Technological Systems and Responsibilities for their Use', in N Bhuta *et al.* (eds), *Autonomous Weapons Systems: Law, Ethics, Policy* (Cambridge University Press, 2016), 39; A Santosuosso, M Tomasi, *Diritto, scienza, nuove tecnologie* (Wolters Kluwer, 2021), 325; NF Frattari, 'Robotica e responsabilità da algoritmo. Il processo di produzione dell'intelligenza artificiale' (2020) 1 Contr. impr. 468.

[31] G Finocchiaro, 'Intelligenza Artificiale e responsabilità' (2020) 2 Contr. impr. 727.

[32] J-S Borghetti, 'How Can Artificial Intelligence Be Defective?', in S Lohsse, R Schulze, D Staudenmayer (eds.), *Liability for Artificial Intelligence and the Internet of Things* (Nomos, 2019), 63,64.

[33] W Barfield, U Pagallo, 'Advanced Introduction' (n 25) 95. See also J Turner, *Robot Rules. Regulating Artificial Intelligence* (Springer, 2019), 218.

[34] It was initially proposed by the European Parliament in the Resolution of 16 February 2017 on civil law rules on robotics.

[35] On the topic, see G. Teubner, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi* (ESI, 2019), Italian version edited by P Femia; Id., 'Digital Personhood? The Status of Autonomous Software Agents in Private Law' (May 11, 2018), available at SSRN: https://ssrn.com/abstract=3177096 or http://dx.doi.org/10.2139/ssrn.3177096; L Arnaudo, R Pardolesi, 'Ecce robot. Sulla responsabilità dei sistremi adulti di intelligenza artificiale' (2023) 4 Danno resp. 415 ff.; F Caroccia, 'Soggettività giuridica dei robot?', in G Alpa (ed), *Diritto e Intelligenza Artificiale* (Pacini Giuridica, 2020), 229; M Laukyte, 'Artificial Agents among Us: Should We Recognize Them as Agents Proper?' (2016) 18(4) Eth. Inf. Tech. 1; T Onida, F Romano, S Santoro, 'Agenti elettronici e rappresentanza volontaria nell'ordinamento giuridico italiano' (2003) 1-2 Inf. dir. 197; LB Solum, 'Legal Personhood for Artificial Intelligences' (1992) 70 North Car. L. Rev. 1231.

[36] Famous in the United States was the study by Curtis E.A. Karnow, who, based on the consideration that 'physical human beings are not the only entities protected by law, nor are they the only entities that have rights', proposed to establish the so-called 'electronic persona' for the artificial agent developed through a comparative judgement with legal persons. See CEA Karnow, 'The Encrypted Self: Fleshing out the Rights

Nevertheless, the elaboration of an *ad hoc* legal personality for software agents has been deemed inappropriate because, from a technical point of view, the state of the art still does not justify giving the software agent a substantive subjectivity of its own,[37] and, from a legal point of view, this would result in a fictitious way to create a separate asset as opposed to the physical persons who effectively control it, who would still be called upon to fund it.[38] Therefore, the attribution of legal personhood to software agents would only be an apparent solution that would complicate legal relations and, in essence, would not solve the complex problem of liability allocation.[39]

On the other hand, it has been suggested that a vicarious liability regime should be applied to damages caused by AI, by assimilating the software agent to an employee for whose actions the employer is accountable, based on the *respondeat superior* model,[40] or to a minor for whom the parents or guardians are responsible.[41] It has either been proposed that the software agent be regarded as an animal for which the owner is accountable.[42] Such proposals, albeit fascinating, do not appear to be feasible insofar as they all tend to attribute to the software agent a degree of subjectivity that does not pertain to it, and, on the other hand, the legal rules corresponding to such liability regimes in the Italian legal system possess special features with respect to the

---

of Electronic Personalities' (1994) 13(1) Journ. Comp. Inf. L. 1. Still in the US, Shawn Bayern demonstrated the possibility for a computer to effectively control a limited liability company, with the consequence that the same AI system could stand trial if the company was sued there. See S Bayern, 'The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems' (2015) 19 Stan. Tech. L. Rev. 93, 112 ff. In a critical sense with respect to Bayern's studies, see Turner, 'Robot Rules' (n 31), 178, 179, according to which 'making decisions on behalf of an entity does not mean having the same legal personality as the entity. A human controller of an LLC therefore does not become personally liable for the debts of the LLC and, presumably, neither does the AI'.

[37] The possibility of suing a machine will only be possible once it has acquired a legal status, which, on closer inspection, will only be possible with the attainment of so-called general AI, because only then will the artificial agent acquire the capacity for litigation, i.e. the capacity to understand not only the meaning of its own actions but also the relevant procedural events. In this respect, see W Barfield, U Pagallo, 'Advanced Introduction' (n 25), 7, 8.

[38] L Coppini, 'Robotica e intelligenza artificiale: questioni di responsabilità civile' (2018) 4 Pol. Dir. 730, 731; A Amidei, 'Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo', in U Ruffolo (ed), *Intelligenza Artificiale e responsabilità. Responsabilità da algoritmo? A.I. e automobili selfdriving, automazione produttiva, robotizzazione medico-farmaceutica. A.I. e attività contrattuali. Le tendenze e discipline unionali* (Giuffrè, 2017), 65 ff.

[39] G Finocchiaro, 'Intelligenza Artificiale e responsabilità' (n 29), 713 ff.

[40] The suitability of such a liability regime is argued based on the relationship between software agent and user, which would be analogous to that which exists between employee and employer, justifying therefore, that the harm caused to third parties should be attributed to those who use makes use of its work and benefits from it. See A Lior, 'AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy' (2020) 46 Mitch. Ham. L. Rev. 1043, 1067 ff.; P Cerka, J Grigiene, G Sirbikyte, 'Liability for Damages Caused by Artificial Intelligence' (2015) 31 Comp. L. Sec. Rev. 385 ff. See also A Beckers, G Teubner, *Three Liability Regimes for Artificial Intelligence. Algorithmic Actants, Hybrids, Crowds* (Hart Publishing, 2021), in which the authors suggest a form of digital vicarious liability similar to a *respondeat superior* hypothesis, in which liability is imputed the user of the system and the imputation criterion is the violation of rules of conduct by the machine.

[41] The analogy between the conduct of a software agent and that of a minor has been argued based on the ability of AI to learn from experience by recording and analyzing data from various sources, including interactions with the user, who would be comparable to a parent. See U Pagallo, *The law of Robots. Crimes, Contracts and Torts* (Springer, 2013), 128, 129; D Marino, G Tamburrini, 'Learning robots and human responsibility' (2006) 6 Int. rev. inf. eth. 46.

[42] The analogy between software agents and animals is supported on the consideration that, like animals, such entities would also be dangerous in that they are unpredictable and inherently irrational. See R Kelley, E Schaerer, M Gomez, M Nicolescu, 'Liability in robotics: an international perspective on robots as animals' (2010) 24(13) Adv. Rob. 1861; Taddei Elmi, Romano, 'Il robot tra ius condendum' (n 14) 127.

relationship existing between the agent and the liable third party, which do not make it appropriate to extend them by analogy outside the cases expressly contemplated therein.[43]

Therefore, it seems appropriate to consider software agents as products or 'things' endowed with evolving and adaptive capabilities. Accordingly, it is necessary to examine those liability regimes that deal with the active role of a product or thing in the causation of harm. Indeed, it has been pointed out that the use of AI in many application domains will cause a shift in focus from human to product, with a resulting predominance for product-focused rather than human-focused liability regimes.[44] Such phenomenon has been observed with regard to some typical sectoral fields of application of tort rules, such as motor vehicle liability[45] and medical liability,[46] where it is possible to experience a progressive erosion of human liability – i.e., that of the driver and of the physician – in favor of that of the producer and/or the person who exerts some sort of supervision on the product. Therefore, in most instances for damages caused by the AI system, its manufacturer and its user will be held liable, alternatively or jointly, based respectively on a malfunction of the system or on the duty to custody of it.

In the Italian legal system, this results in the need to assess the enduring enforceability of the rules designed to regulate such cases with respect to the features of autonomy and unpredictability of the intelligent software agent. In this view, it is necessary to reject the idea that the starting question is 'who' and 'why' someone should be liable for AI-related torts, thus neglecting the rigid dichotomy fault-strict liability. In fact, in Italian tort law there is a plurality of liability criteria, each responding to a different rationale depending on the context in which the damage occurs and having variable degrees of objectivity.[47] The inherently dynamic and evolving nature of AI requires to adhere to and to reaffirm such a flexible liability paradigm.

---

[43] Ruffolo, 'Intelligenza artificiale, machine learning' (n 14) 1698 ff.; Bertolini, 'Robots as products' (n 12) 227, 228; M Bassini, L Liguori, O Pollicino, 'Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?', in F Pizzetti (ed), *Intelligenza Artificiale, protezione dei dati personali e regolazione* (Giappichelli, 2018), 359 ff.

[44] G Calabresi, E Al Mureden, *Driverless cars. Intelligenza artificiale e futuro della mobilità* (il Mulino, 2021), 147 ff.

[45] It has been often pointed out that as vehicles become more autonomous, civil liability will progressively shift from the driver to the producer. In this respect, see MC Gaeta, 'Automazione e responsabilità civile automobilistica' (2016) 5 Resp. civ. prev. 1718 ff.; E Al Mureden, 'Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo' (2019) 3 Contr. impr. 911 and, more recently, MC Gaeta, 'Civil liability rules for autonomous vehicles accidents in Italy', in H Steege, IA Caggiano, MC Gaeta, B Von Bodungen (eds), *Autonomous Vehicles and Civil Liability in a Global Perspective. Liability law study across the world in relation to SAE J3016 Standard for Driving Automation* (Springer, 2024) 371; T De Mari Casareto dal Verme, 'Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma' (2023) 3 Biol. Journ. 275 ff. For a comprehensive and in-depth study of the relationship between self-driving cars and civil liability, see MC Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies* (Editoriale Scientifica, 2019, reprint 2023).

[46] In the healthcare sector, it has been observed that the higher the autonomy of the AI system in making healthcare treatment decisions, the less the physician should be liable for damages caused by the algorithm and, therefore, the greater the role of the liability of the medical software manufacturer. For deeper insights, see M Faccioli, 'Intelligenza artificiale e responsabilità sanitaria' (2023) 3 Nuova giur. civ. comm., 732; G Votano, 'Intelligenza artificiale in ambito sanitario: il problema della responsabilità civile' (2022) 6 Danno resp., 673.

[47] On the topic, S Rodotà, *Il problema della responsabilità civile* (Giuffrè, 1967), 144 ff.; R Scognamiglio, 'Responsabilità per colpa e responsabilità oggettiva', in Aa Vv, *Studi in memoria di Andrea Torrente* (Giuffrè,

5. The liability of the manufacturer.

On the production side, the applicability of the PLD, as transposed into the Italian legal system,[48] comes into play as the main liability regime to be invoked in cases of AI-related torts. In this respect, it has been questioned whether the PLD was applicable to defective AI systems, since it was first disputed whether AI software falls within the notion of 'product' and, consequently, whether its creator could be considered to be a producer within the meaning of the Directive.[49]

We consider this question positively resolved because, on the one hand, we agree with the interpretation of the current PLD in the sense that it already covers software as a product,[50] and, on the other hand, the new version of the Directive now expressly treats software as a product to which this liability regime applies. It is possible, therefore, to assert the applicability of the PLD both to cases where the AI software is placed on the market independently and where it constitutes a component of a final tangible or intangible product. In any case, the consumer will not necessarily have to identify the producer of the specific defective component but may sue whoever presents themselves as the producer or places their trademark on the product.[51]

Nevertheless, the victim must fulfil the burden of proof set by Article 4 of the previous PLD – confirmed by Article 10 of the new Directive – according to which the injured person shall be required to prove the damage, the defect and the causal relationship between defect and damage. Such burden of proof operates regardless of the (only possible) alleviation mechanisms provided therein. In this regard, it has often been pointed out that the technical sophistication of modern AI systems would not allow the injured party to meet their burden of proof, especially with regard to the proof of defect.[52] This

1968), 1123; C Castronovo, *La nuova responsabilità civile. Regola e metafora* (Giuffrè, 1991), 8; C Salvi, *La responsabilità civile* (Giuffrè, 2019), 161 ff.

[48] The PLD was first transposed in the Italian legal system with the D.P.R. 24 May 1988, n. 224, then incorporated into the Consumer Code (D.lgs. 6 September 2005, n. 206).

[49] This issue arises from the debate about whether software qualifies as a product or as a service, in which latter case the PLD would not be applicable whenever, for example, the software is supplied on demand and made customized by the applicant and not in series. See Barfield, Pagallo, 'Advanced Introduction' (n 25), 11,12; A Zaccaria, 'La responsabilità del «produttore» di software' (1993) Contr. impr. 303 ff.; CL Williams, 'Not so Good: The Classification of Smart Goods Under UCC Article 2' (2018) 34 Georg. St. Un. L. Rev. 453.

[50] R Montinaro, 'Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law' (2020) 4 Pers. merc. 372; Ruffolo, 'Intelligenza artificiale, machine learning' (n 14) 1691.

[51] It was otfen pointed out that the person harmed by a smart product would face difficulties in detecting the specific subject against whom to direct a legal proceeding, due to the technical sophistication characterizing such devices that are made by many different components, and it is complex to attribute the defect to one of them. In practice, this obstacle can be bypassed since the PLD establishes a regime of joint and several liability among the different actors of the production chain, whereby the consumer is not burdened with identifying the 'real producer', but can take legal action against any of the parties who present themselves as such or who place their own trade mark or other distinctive sign on the product, thus burdening the production chain with the risk of identifying the 'weak link' of the chain. For such a conclusion, see the decision of the Court of Justice of the European Union, Case C-264/21, *Keskinäinen Vakuutusyhtiö Fennia v Koninklijke Philips NV*, 7 July 2022 (ECLI:EU:C:2022:536).

[52] On the topic, see C Scognamiglio, 'Responsabilità civile ed intelligenza artificiale' (n 12) 1084; GF Simonini, 'La responsabilità del fabbricante nei prodotti con sistemi di intelligenza artificiale' (2023) 4 Danno resp. 435 ff.; Montinaro, 'Responsabilità da prodotto difettoso' (n 46) 365; A Procida Mirabelli di Lauro, 'Le intelligenze artificiali tra responsabilità civile e sicurezza sociale', in Perlingieri, Giova, Prisco (eds), 'Rapporti civilistici e intelligenze artificiali' (n 12) 329, 330; C Amato, 'Product Liability and Product Security: Present and Future',

aspect is of central importance since the usability of the proof of the defect translates into the concrete possibility for those damaged by defective products to have access to justice, since case law identifies the product's defect as the indefectible prerequisite of producer liability.[53]

On the defendant's side, these problems result in the possibility that the harm caused by a self-modifying algorithmic decision could lead to the automatic application of the 'later-defect defense' and of the 'state-of-the-art defense', creating a form of producer immunity from liability,[54] which is not desirable for several reasons[55] and exacerbates the mentioned responsibility gap.

5.1. The proof of defectiveness: the 'model software agent'.

Within the PLD the defectiveness of the product represents the criterion for assessing manufacturer's liability and it must be proved by the claimant. According to Article 6 of the PLD (Article 7 of the new PLD), a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account. As such, the EU legislator did not adhere to the U.S. model – which explicitly defined the well-known categories of manufacturing, design and information defect –[56] but outlined a unitary notion of defect based on the so-called 'consumer expectations test'. The concept of defect under the Directive functions as a general and flexible clause,[57] rooted in the public's legitimate safety expectations.

That of defect, thus, is a relational concept rather than a technical one,[58] i.e., the defectiveness of the product must be assessed in the light of the relationship between the actual functioning of the product and the safety that the public at large was reasonably entitled to expect taking all circumstances into account. In this respect, Italian case law[59] affirms that it is not required that

---

in Lohsse, Schulze, Staudenmayer (eds.), 'Liability for artificial intelligence' (n 30) 79 ff.; HR Sullivan, SJ Schweikart, 'Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?' (2019) 21 AMA Journ. Eth. 160.

[53] In the case law, see e.g. Cass. civ. sez. III, 19 February 2016, nr. 3258; Trib. Sulmona, 23 October 2010, nr. 501.

[54] R Calo, 'Open Robotics' (2011) 70 Mar. L. Rev. 571.

[55] For deeper insights, see E Palmerini, 'AI Systems and the Issue of Liability in the European and National Regulatory Strategies', in P Morgan (ed), *Tort Liability and Autonomous Systems Accidents* (Edward Elgar, 2023), 73 ff.

[56] In the US legal system, the distinction between manufacturing defects, design defects and information defects has been formalised by the Restatement of Torts, Third, at § 2, published in 1997. In the former case, strict liability is imposed on the producer and the seller, without prejudice to actions of redress between the two. In the second, the risk/utility test is adopted in order to assess the producer's liability. Finally, the producer's liability for missing information and warnings should only arise if the information or warnings would have enabled the user of the product to avoid or reduce the risk of occurrence of that damage.

[57] C Scognamiglio, 'Clausole generali e linguaggio del legislatore: lo standard della ragionevolezza nel D.P.R. 24 maggio 1988 n. 224' (1992) Quadr. 65 ff.; Montinaro, 'Difetto del prodotto, norme tecniche' (n 10) 281; GF Simonini, 'L'approccio olistico nel danno da prodotto' (2018) 2 Danno resp. 138.

[58] F Cafaggi, 'La nozione di difetto ed il ruolo dell'informazione. Per l'adozione di un modello dinamico-relazionale di difetto in una prospettiva di riforma' (1995) Riv. crit. dir. priv. 447 ff. See also J Meltzer, R Freeman, S Thomson, in *Product liability in European Union: a report for the European Commission*, 2003.

[59] See Cass. civ. sez. III, 8 October 2007, nr. 20985, where the Court of Cassation noted that the injured party is not required to prove the specific defect of the product, it being sufficient to prove those facts, pertaining to its use, from which it is possible to derive an assessment of its unsafety. See also Cass. civ., sez. III, 15 February 2018, nr. 3692.

the consumer prove the specific material defect affecting the product, sometimes interpreting the defect as a failure to comply with the standards of reliability required by users or by the relevant laws on the subject.[60] In fact, according to the principle of proximity of evidence,[61] an inherent design or manufacturing defect is unlikely to be within the consumer's power of appreciation, so that the burden of proof is distributed among parties taking into account the concrete possibility for the plaintiff and the defendant to prove facts and circumstances falling within their respective spheres of action.[62] This is confirmed by the fact that expert opinion within the trial, although useful, is not essential to prove the defect of the product,[63] also considering that often the defective product that caused the damage goes destroyed in the event of the accident and that a direct analysis of it is not feasible.[64]

Ultimately, the assessment of the defectiveness of the product depends largely on the claimant's ability to demonstrate factual circumstances from whose overall evaluation the court may validly infer such character.[65] From this point of view, the assessment of the product's defectiveness before the Courts often builds on the manner in which the event occurred together with the characteristics of the product as perceived externally by the injured party in its appearance,[66] in relation to an assessment of the reasonable expectations.[67] To do so, according to the above-mentioned relational model, the defectiveness of the product can be derived by comparing the product's external characteristics and functioning with a hypothetical, abstract model of a safe product that embodies the reasonable expectations of the public at large. Where such an argument results in a divergence between the functioning of the actual product and that of the model, the defect proof will be deemed to have been satisfied.

---

[60] Cass. civ., sez. III, 29 May 2013, nr. 13458.

[61] The principle of proximity of evidence constitutes a criterion that is sometimes supplementary and sometimes an alternative to the general rule on the distribution of the burden of proof, in so far as it helps the court to seek the solution best suited to ensuring the effectiveness of judicial protection by placing the burden of proof on the person who has the easiest access to the knowledge of relevant information and facts. See R Rordorf, 'Onere della prova e vicinanza della prova' (2023) 1 Jus Civile. 11 ff.; M Franzoni, 'La «vicinanza della prova», quindi…' (2016) 2 Contr. impr. 360 ff.; G Vettori, 'Il diritto ad un rimedio effettivo nel diritto privato europeo' (2017) 3 Riv. dir. civ. 670. In case law, the principle has been enshrined in the famous judgment Cass. civ. sez. un., 30 October 2001, nr. 13533.

[62] On the application of the principle of proximity of evidence to product liability, see A Genovese, 'Responsabilità del produttore' (2013) Dig. disc. priv., sez. civ., 614; A Di Majo, 'La responsabilità per prodotti difettosi' (1989) 1 Riv. dir. civ. 34. Within the case law, see *inter alia* Trib. Cuneo, 17 December 2021, nr. 1071

[63] The results of technical expert opinion are not always sufficient to offer the unequivocal demonstration of the product's lack of the safety that the public is entitled to expect, since scientific evidence is not a proper proof, but merely an aid for the judge in assessing the facts and making a decision. On the topic, see A Fusaro, 'Responsabilità del produttore: la difficile prova del difetto' (2017) 6 Nuova giur. civ. comm. 898.

[64] F Raspagni, 'Responsabilità del produttore: ripensamenti e conferme in tema di onere della prova del difetto – il commento' (2015) 10 Danno resp. 958.

[65] G Stella, 'Causa ignota del danno derivante dall'uso del prodotto e responsabilità del produttore per prodotto difettoso' (2017) 5 Resp. civ. prev. 1457.

[66] G Alpa, M Bessone, *La responsabilità del produttore* (Giuffrè, 1999), 339.

[67] Case law and scholars highlight the role of the reasonable principle in the assessment of the defect, which in the Italian transposition of the PLD was translated in the word 'legitimately' (*legittimamente*). See *inter alia* Cass. civ., sez. III, 13 August 2015, n. 16808; U Carnevali, 'Prevenzione e risarcimento nelle direttive comunitarie sulla sicurezza dei prodotti' (2005) 1 Resp. civ. prev. 12.

When it comes to torts committed by intelligent software agents the described operational rules may function, still taking into account the peculiarities of such sophisticated products. In fact, the liability regime under the PLD presents itself sufficiently flexible to cover also the complexity of AI: the primary rationale of the Directive was to strike a balance between consumer protection and incentivizing technological innovation, and it does so by outlining the defect as a general and flexible clause rather than a technical notion. In this view, we hereby provide for a proposal for applying the above-mentioned relational model to smart products as well.

First of all, the product's ability to evolve and the unpredictability of its harmful decisions do not affect the burden of proof on the injured person. Indeed, it is not required to the claimant to demonstrate that the defect traces back to the production phase, since it lies on the defendant to prove the 'later-defect' in order to escape liability.[68]

Second, when it comes to products endowed with highly sophisticated learning capabilities, it must be ruled out that the injured party should have to prove the specific deficiency in the internal decision-making process of the algorithm, just as the 'traditional' injured parties are not required to prove the specific material defect that caused the damage. The injured party will be entitled to fulfil their burden of proof by referring to the manner in which the event occurred together with the characteristics of the product as externally perceivable, in accordance with the described principle of proximity of evidence. [69] In this view, it should be considered that one of the main characteristics of an intelligent software agent is that it makes decisions which manifest themselves as externally perceivable behaviors. Accordingly, the conduct of the product as perceived by the claimant will be subject to evaluation in order to assess its defectiveness.[70] It is therefore appropriate to overcome the assumption that the defect should only refer to the properties of the product and not also to its 'behaviour'.[71]

The assessment of defectiveness may be based on the deviation of the software agent's external behavior from the conduct ideally performed by a hypothetical 'model software agent',[72] similarly to what happens with the assessment of fault under Article 2043 of the Civil Code, which has now

[68] G Stella, 'Causa ignota del danno' (n 60) 1450 ff.

[69] Of the same opinion is Montinaro, 'Responsabilità da prodotto difettoso' (n 46) 385, who observes that when establishing the defectiveness of an IA system it is appropriate to employ the principle of proximity of evidence in order to distribute the burden of proof among the parties to the proceedings, in the direction of a system inspired by the effectiveness of protection so as not to make access to remedies impossible for the injured party.

[70] The appropriateness of electing the external behaviour of the system as a reference parameter for defectiveness is recognized by those who emphasize the need to carry out this assessment by means of a concrete and ex post judgement aimed at evaluating the misalignment of the product's behaviour with the standards that the user community is reasonably entitled to expect. In this respect, see Procida Mirabelli di Lauro, 'Le intelligenze artificiali' (n 48) 315. See also Beckers, Teubner, 'Three Liability Regimes' (n 38), who reconstruct the AI liability model on the basis of the violation of rules of conduct by the machine.

[71] In this respect, see G Borges, 'Liability of the Operator of AI Systems De Lege Ferenda', in S Lohsse, R Schulze, D Staudenmayer (eds), *Liability for AI. Munster Colloquia on EU Law and the Digital Economy VII* (Nomos, 2023) 171, observes that 'the concept of defect refers to the properties of the product, not to its behaviour'.

[72] For deeper insights, please refer to De Mari Casareto dal Verme, 'Intelligenza Artificiale e responsabilità civile' (n 27), 251 ff.

assumed an objective nature.[73] To do so, the model will reflect the reasonable expectations of the public at large with regard to an ideally safe conduct of the product. Such a model will vary according to the actual features of the product, the context in which it is employed, its relationship with the user, and so on, taking all circumstances into account and employing the 'reasonableness' principle[74] as a filter to constrain the possible overreaching of the parameter.[75]

Such a proposal does not differ very much from applying the *res ipsa loquitur* principle also to AI-related torts. This principle is already well-known in the legal environment and consists in the employment of presumptions to prove usually the fault[76] of an agent or the defectiveness of a product[77] by alleging facts that 'speak for themselves'. When it comes to a smart product, as a thing that really can speak for itself, the *res ipsa loquitur* principle may allow to infer the product's defectiveness – and, thus, the producer's liability – by demonstrating a 'negligent' conduct of the software agent which did not comply with the public's safety expectations.[78]

5.2. The defenses.

Once the injured party has met their burden of proof, it is up to the manufacturer to prove at least one of the circumstances listed in Article 11 of the PLD if they wish to escape liability. As already mentioned, the features of the intelligent software agent might create problems with two specific defenses – the 'later-defect defense' and the 'state-of-the-art defense' – since

[73] Fault-based liability in the Italian legal system is nowadays given an objective interpretation, in the sense that the assessment of fault does not look at the agent's subjective blame but is based on the objective deviation of the conduct of the liable party from the conduct of a hypothetical model agent complying with the rules of diligence required by the circumstances or by specific laws or regulations. See inter alia M Franzoni, L'illecito (Giuffrè, 2010), 175 ff.

[74] In this respect, see also MC Buiten, 'Product liability for defective AI' (2024) 57 Eur. Journ. L. Econ., 259 ff., who observes that in case of smart products 'under EU product liability law, courts will have to judge the reasonableness of the public's inaccurate expectations of AI'.

[75] The principle of reasonableness is now part of the daily work of judges, as its flexibility allow them to invoke it for emancipating judicial decisions from the syllogistic and literal application of the law and to adapt them to the demands of equity, fairness and justice of the individual case. At the same time, when the principle is explicitly enshrined in a legal norm (as it happened with product liability in the Italian Consumer Code), it contributes to constrain the possible judge's excessive discretion. On the topic, see G Perlingieri, 'Sul criterio di ragionevolezza', in G Perlingieri, A Fachechi (eds), *Ragionevolezza e proporzionalità nel diritto contemporaneo* (vol I ESI, 2017), 6; S Patti, *La ragionevolezza nel diritto civile* (Editoriale Scientifica, 2012), 18; A Ricci, *Il criterio della ragionevolezza nel diritto privato* (Cedam, 2007), 42.

[76] The principle of res ipsa loquitur represents a method of simplifying the burden of proof that originates in common law case law – with particular regard to *Byrne v. Boadle*, 159 Eng. Rep. 299, 300 (Ex. 1863) – dealing with the proof of fault in all those cases where the harmful event presents itself with such striking peculiarities as to 'speak for itself' about the negligence of the agent and to justify a reversal of the burden of proof. On the topic, see BS Markesinis, SF Deakin, *Tort Law* (Oxford University Press, 1999), 171 ff.; U Izzo, *La precauzione nella responsabilità civile* (Cedam, 2004), 131 ff. In the Italian legal system, it found particular application in cases of medical liability. See V Fineschi, 'Res ipsa loquitur: un principio in divenire nella definizione della responsabilità medica' (1989)2 Riv. it. med. leg. 419 ff. In the Italian case law, see Cass. civ., sez. III, 21 December 1978, nr. 6141; Cass. civ., sez. III, 22 January 1999, nr. 598; Trib. Napoli, 3 December 2014, nr. 15998; Trib. Roma, 17 November 2014, nr. 22866.

[77] On the applicability of the *res ipsa loquitur* principle to product liability, see Procida Mirabelli di Lauro, 'Le intelligenze artificiali' (n 48) 320; Montinaro, 'Difetto del prodotto, norme tecniche' (n 10) 284 ff.

[78] See R Casey, 'Robot Ipsa Loquitur' (2019) 108 Georg. L. Journ. 225, on the applicability of the *res ipsa loquitur* principle to torts committed by AI. In fact, not being necessary to prove the 'wrong code line', 'thanks to *res ipsa loquitur*, plaintiffs involved in automated accidents can rely on inference to establish fault, even when they lack direct insight into the system's underlying code'.

the learning and evolving capabilities of the software agent could lead to an automatic application of such exemptions, thus depriving the injured party of substantive access to justice. We hereby provide for an interpretation of the mentioned defenses able to prevent such a result.

As regards the 'later-defect defense', according to Article 11(c) of the new PLD the producer shall not be liable if they prove 'that it is probable that the defectiveness that caused the damage did not exist at the time the product was placed on the market, put into service or, in the case of a distributor, made available on the market, or that that defectiveness came into being after that moment'. In AI-related torts, if the damage was caused by a behaviour resulting from self-modification of the product after its deployment, such a defect could automatically be regarded as supervening and the producer would always escape liability.[79] Nevertheless, in the Italian legal system, this conclusion does not seem to be supported.

In light of the difficulty for the producer to supply negative proof of the absence of an initial defect, case law and doctrine interpret this exemption as meaning that the producer will have to supply positive proof that the defect was caused by circumstances external to and subsequent to the product's being put into circulation, such as its manipulation by third parties.[80] Thus, the defense cannot be interpreted as meaning that the product's learning capacity is *per se* capable of exempting producer's liability, since the latter is required to prove that the defect originated exclusively from a source external to the product and beyond the producer's control.[81] Nevertheless, under the new paragraph 2 of Article 11, by way of derogation the abovementioned letter (c), an economic operator shall not be exempted from liability where the defectiveness of a product is due to software, including software updates or upgrades, provided that the product is within the manufacturer's control.

As regards the 'state-of-the-art defense', according to Article11(e) of the PLD the producer shall not be liable if he proves 'that the objective state of scientific and technical knowledge at the time the product was placed on the market or put into service or during the period in which the product was within the manufacturer's control was not such that the defectiveness could be discovered'. When it comes to AI systems, the possible unpredictability of the harmful output could automatically exclude producer's liability,[82] since the defense is intended to limit producer's liability to defects that were foreseeable by the producer at the moment he placed the product on the market.

Nevertheless, the unpredictability of the defect must be read not in the light of the impossibility for the individual producer to discover the defect, but in an objective sense, i.e. according to the most advanced knowledge in all fields of

[79] S Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the law* (Cambridge University Press, 2021), 96, notes that with more advanced AI systems, particularly those with the ability to modify themselves, the manufacturer could invoke as contrary evidence that the defect did not exist at the time the product was put into circulation. In the same sense, M Ratti, 'Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo' (2020) 3 Contr. impr. 1174.

[80] G Stella, 'Causa ignota del danno' (n 60) 1449 ff.

[81] Sometimes such defense has been interpreted as similar to force majeure. See Alpa, Bessone, 'La responsabilità del produttore' (n 61) 259.

[82] Procida Mirabelli di Lauro, 'Le intelligenze artificiali' (n 48) 325.

science and technology.[83] Thus, the exemption only covers risks that are absolutely unforeseeable because they are absolutely unknown.[84] Therefore, the mere ability to learn, which is present in the product since its conception, can certainly not *per se* ground exemption from liability for the manufacturer, the latter having to prove the absolute unpredictability of the product's defective behaviour in the light of all the technical knowledge available at the time of its release. Then the applicability of the exemption will also be subject to an assessment of the behaviour of the AI system as totally deviating from what is reasonably foreseeable according to the state of the art, taking all circumstances into account. The development risk, then, must also be subsumed into the relational model, informed by the standard of what the producer could reasonably foresee. In this view, the reasonableness principle is capable of both defining and limiting producer's liability.[85]

6. The liability of the user: the 'custody' over the software agent.

On the user side, in Italian tort law the liability regime destined to take a central role in AI-related torts is that set forth in Article 2051 of the Civil Code, according to which for damage caused by a thing the keeper thereof shall be liable, unless he proves fortuitous. It is a strict liability regime designed to hold liable whoever exerts custody over a thing that causes damage to third parties, meaning that the injured person shall not prove that the custodian was in fault but only the causal relationship between the think and the damage.

When it comes to AI systems, it has been pointed out that the conditions for liability under Article 2051 would not be compatible with the characteristics of modern AI, due to the limited possibility of control over the software agent by the user caused by the former's ability to make decisions autonomously and to perform actions unforeseeable by that subject.[86] In other words, it would not be possible to exert custody over the intelligent software agent.[87]

First of all, it should be clarified whether the software agent falls within the notion of 'thing' under Article 2051, since the Civil Code does not provide for a definition of it. In case the AI software is a component of a physical object, there is no doubt that Article 2051 is applicable. Otherwise, we should conclude that a thing is not a thing every time its functioning is software-based. On the

[83] The reference goes to the Judgment of the Court (Fifth Chamber) of 29 May 1997, *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland*, C-300/95, in which the European Commission clarified that the Directive does not refer to a producer's ability to discover the defect on the basis of his own knowledge, but to an objective state of knowledge not limited to a specific field.
[84] R Montinaro, *Dubbio scientifico e responsabilità civile* (Giuffrè, 2012), 110 ff.
[85] For deeper insights, please refer to De Mari Casareto dal Verme, 'Intelligenza Artificiale e responsabilità civile' (n 27), 286 ff.
[86] G Sartor, 'Gli agenti software: nuovi soggetti del ciberdiritto?' (2016) 2 Contr. impr. 465; Bassini, Liguori, Pollicino, 'Sistemi di Intelligenza Artificiale' (n 41) 333 ff.; Matthias, 'The Responsibility Gap' (n 11) 175 ss.; JKC Kingston, 'Artificial Intelligence and Legal Liability', in M Brame, M Petridis (eds), *Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV* (Springer, 2016), 269 ff.
[87] See M Franzoni, 'La responsabilità civile: una lunga storia ancora da scrivere' (2021) 4 Contr. impr. 1121, who expresses doubts about the applicability of Article 2051 to AI systems. See also V Di Gregorio, 'Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?' (2022) 1 Danno resp. 58; M Costanza, 'L'Intelligenza Artificiale e gli stilemi della responsabilità civile' (2019) 7 Giur. it. 1687.

contrary, when the software agent causes damages independently, more questions arise. In this respect, it seems that the notion of 'thing' under Article 2051 has been interpreted in a broad sense, encompassing also non-material entities.[88] Furthermore, the legal nature of software has been long debated and today is generally accepted that software is an entity susceptible of being possessed.[89] To support this conclusion, the concept of 'thing' should be interpreted in the light of a systematic reading of Article 2051 and Article 810, which is sufficiently broad to also include non-tangible realities for which, e.g., possession is admitted.

Accordingly, there are no valid reasons why not to consider software a thing susceptible of being under the custody of a natural or legal person.

Second, it seems that the notion of 'custody' under Article 2051 is compatible with the features of modern AI. In fact, the norm is interpreted as establishing a strict liability regime where the 'custody' does not refer to control over the thing, but it is a *de facto* relationship between the thing and the custodian that implies the possibility of avoiding the harmful consequences connected with it.[90] Custodian is, therefore, anyone who is in a position to decide and govern the conditions of use and maintenance of the thing.(264)[91] The rationale of the norm lies on the 'cheapest-cost-avoider' principle, regardless of the custodian's possibility of controlling the thing or of the unpredictability of its functioning. The main function of the rule, then, is precisely to secure compensation to the injured party even when the thing escapes human control and releases its power in an unforeseen direction or to an unforeseen extent.[92]

7. Conclusions.

The analysis carried out shows that Italian tort law is equipped with sufficiently flexible and dynamic tools to allow the existing rules to cover also cases of damages caused by intelligent software agents, albeit with the appropriate interpretative adjustments.

On the production side, the relational concept of defect makes it possible to reaffirm the functioning and rationale of the PLD as a compromise between consumer protection and the need not to discourage technological progress, with a view to ensuring a common market in which all economic actors can benefit from innovation. At the same time, for this to happen it is necessary to accept the probability that there is an ineliminable portion of risk corresponding to torts that, at least in the near future, may remain without

[88] The concept of 'thing' under Article 2051 is often interpreted to mean any inanimate element, whether movable or immovable, solid but also liquid or gaseous. See A Leonardi, '(L'accidentato terreno del) Danno da cose in custodia' (2018) 5 Resp. civ. prev. 1568; GG Greco, DM Pasanisi, B Ronchi, *I danni da cose in custodia* (Giuffrè, 2004), 51; P Zivis, 'Il danno cagionato dalle cose in custodia' (1989) 2 Nuova giur. civ. comm. 100.

[89] In this respect, see AC Nazzaro, 'Nuovi beni tra funzione e dogma' (2013) 4-5 Contr. impr., 1017, who observes that the dominant opinion sees intangible assets such as software, databases, know-how and websites as entities susceptible to possession.

[90] Within the case law, see *inter alia* Cass. civ, sez. III, 29 September 2017, nr. 22839; Cass. civ., sez. III, 29 July 2016, nr. 15761.

[91] Cass. civ., sez. III, 8 February 2012, nr. 1769; Cass. civ., sez. III, 19 May 2011, nr. 11016.

[92] P Trimarchi, *Rischio e responsabilità oggettiva* (Giuffrè, 1961), 196.

compensation. Indeed, it is natural that the introduction of technological innovations into society entails an inevitable period of adjustment necessary for the elaboration of legitimate user expectations. But in reality, the existence of a 'free zone', where the cost of damages remains where they occurred, is a risk that is always necessary to enable technological innovation.

On the user side, the legal system appears to be inspired by the idea of burdening the risk of damage on the subject placed in the best situation to prevent it, by allowing the injured party to sue the person to whom the harmful event can most immediately be traced back to, due to the risk factor introduced into the society by the thing over which they exert custody.

SECTION III

FOCUS PAPERS

Gatt L, Caggiano IA, Gaeta MC, Troisi E, Savella R, Pratesi F, Trasarti R, 'FRIA implementation model according to the AI Act' (2024) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT242LGIACMCGETRSRTFP

EJPLT
ISSN 2704-8012



FRIA implementation model according to the AI Act

Modello di attuazione FRIA in applicazione dell'AI Act

Lucilla Gatt
Full professor of Private Law, Director of the Research Centre in European Private Law (ReCEPL) Suor Orsola Benincasa University of Naples

Ilaria Amelia Caggiano
Full professor of Private Law, Vice-Director of the Research Centre in European Private Law (ReCEPL)
Suor Orsola Benincasa University of Naples

Maria Cristina Gaeta
Lecturer in Private Law, Ph.D., Scientific Secretary of the Research Centre in European Private Law (ReCEPL)
Suor Orsola Benincasa University of Naples

Emiliano Troisi
Ph.D., Junior Researcher Research Centre in European Private Law (ReCEPL),
Suor Orsola Benincasa University of Naples

Roberta Savella
Research Fellow Project SoBigData++
Institute of Information Science and Technologies "Alessandro Faedo" (ISTI),
National Research Council

Francesca Pratesi
Researcher Project SoBigData++
Institute of Information Science and Technologies "Alessandro Faedo" (ISTI),
National Research Council

Roberto Trasarti
Researcher Project SoBigData++
Institute of Information Science and Technologies "Alessandro Faedo" (ISTI),
National Research Council

Abstract
The paper presents the FRIA project aimed at researching and specifying a methodology to assess the impact of Artificial Intelligence (AI) systems on fundamental rights, as recognised by the international and European regulations of hard law and soft law, with the specific reference to the judicial sector as the field of analysis. The research methodology starts from the study of the existing legal and ethical frameworks concerning AI and human rights and the translation of the identified rules and principles into a set of synthetic requirements to create an automated risk assessment methodology. The research output is a prototype tool to support and automate the fundamental rights impact assessment of high-risk AI systems, which is in line with the requirements of the European Artificial Intelligence Act.

* The paper is the result of the work of a selected team of researchers of the Research Centre in European Private Law (ReCEPL), coordinated by the ReCEPL Director Prof. Lucilla Gatt and ReCEPL Vicedirector Prtof.ssa Ilaria A. Caggiano, as well as the National Research Council of Italy, coordinated by CNR First Researcher Doc. Roberto Trasarti. This work is supported by the European Union – Horizon 2020 Program under the scheme "INFRAIA-01-2018-2019 – Integrating Activities for Advanced Communities", Grant Agreement n.871042, "SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics" (http://www.sobigdata.eu), and NextGenerationEU – National Recovery and Resilience Plan (Piano Nazionale di Ripresa e Resilienza, PNRR) – Project: "SoBigData.it – Strengthening the Italian RI for Social Mining and Big Data Analytics" – Prot. IR0000013 – Avviso n. 3264 del 28/12/2021.

© The author(s) 2024, 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 lavoro presenta il progetto FRIA finalizzato alla ricerca e alla specificazione di una metodologia di valutazione dell'impatto dei sistemi di Intelligenza Artificiale (IA) sui diritti fondamentali, così come riconosciuti dalle normative internazionali ed europee di hard law *e* soft law*, con specifico riferimento al settore giudiziario come ambito di analisi. La metodologia di ricerca parte dallo studio dei quadri giuridici ed etici esistenti in materia di IA e diritti umani e dalla traduzione delle norme e dei principi identificati in un insieme di requisiti sintetici per creare una metodologia di valutazione automatica del rischio. Il risultato della ricerca è un prototipo di strumento per supportare e automatizzare la valutazione dell'impatto sui diritti fondamentali dei sistemi di IA ad alto rischio, in linea con i requisiti del Regolamento europeo sull'intelligenza artificiale.*

Keywords: AI Act; high-risk AI systems; impact assessment; FRIA; metrics methodology; ELS; risk management; Law&Ethics

Summary: 1. Introduction and background. – 2. Methodology. – 3. State of the art. – 3.1. International and European existing legal and ethical framework concerning AI and human rights. – 3.2. Italian state of the art AI regulation, with specific reference to its impact on human rights. – 4. Cyberjustice and FRIA: Integrating AI in Judicial Contexts. – 5. Objectives. – 6. The analytical process. – 7. Experiment design. – 8. Conclusions.

1. Introduction and background.*

In the AI regulation at a European and international level, the idea of ex ante protection as the main protection in relation to high-risk AI systems has been consolidated and a risk-based approach has been selected to measure the risk of damages resulting from the different AI applications.

The definition of AI system is currently provided by the Artificial Intelligence Act (Reg. 2024/1689/EU - AI Act), art. 3, para 1, no. 1, as a machine-based system designed to operate with different levels of autonomy and that may exhibit adaptiveness after deployment. Moreover, AI systems produce outputs (predictions, contents, recommendations or decisions) from the input received, that can influence physical or virtual environments. The AI Act classifies AI systems according to their possible risks for individuals, providing a specific regulation for high-risk AI systems (art. 6 ff. AI Act).

High-risk AI systems are defined as systems used as security components of a product or security products themselves, that are required to undergo a third-party conformity assessment (art. 6, para 1 AI Act). In addition, AI systems referred to in Annex III shall be considered to be high-risk, such as those related to the administration of justice listed at no. 8, Annex III, AI Act.

* The work was presented at the IEEE International Conference 'Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering' (MetroXRAINE), St Albans, London, October 21-23, 2024, and published in the IEEE MetroXRAINE 2024 Proceedings, 1224 – 1229.
The authors of this paragraph are Dr. Maria Cristina Gaeta and Dr. Emiliano Troisi.

aims to prevent human rights violations and serve as an accountability tool for risk management system and impact assessment.

However, currently, no complete tools have been implemented with which to proceed to achieve this preventive protection. Indeed, there are mainly tools based on a self-assessment system, also provided by public entities, like the ALTAI (Assessment List for Trustworthy Artificial Intelligence)[1], a prototype of a tool to support AI R&D based on 7 ethical guidelines presented in 2020 by the High-Level Expert Group on Artificial Intelligence (AI HLEG). In the same direction, Council of Europe's European Commission for the Efficiency of Justice (CEPEJ) elaborated in 2023 the Assessment tool for the operationalisation of the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment which consists of 29 questions. Furthermore, the CEPEJ Assessment Tool seems to be complementary to the Human Rights, Democracy, and the Rule of Law Impact Assessment (HUDERIA)[2], which is currently being designed by the Council of Europe's Ad Hoc Committee on AI (CAHAI), as uniform model for human rights impact assessments (HRIAs) of AI systems meeting the parameters and supporting the application of the recent approved Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law of 2024.

At the national level, instead, could be mentioned the FRAIA tool, elaborated by the Government of the Netherlands to help in mapping the risks to human rights in the use of algorithms and to take measures to address these risks[3]. These systems do not guarantee an overall view of fundamental rights, but rather take only certain aspects into account, lacking a comprehensive analysis necessary to ensure effective protection of the individuals, especially in risk-specific deployment contexts. Because of the lack of an effective tool suitable for the purpose of assessing the impact of AI on fundamental rights in a quantifiable, automatic and objective way, evaluation errors may occur which can then result in excessive or unexpected costs for individuals and companies.

Starting from the consequences of AI on human rights [4] and the introduction of the FRIA regulation in the AI Act, this study comes from the

[1] High-Level Expert Group on Artificial Intelligence, Assessment List for Trustworthy Artificial Intelligence (ALTAI), 17 of July 2020, freely available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[2] Council of Europe's Ad Hoc Committee on AI (CAHAI), Human Rights, Democracy, and Rule of Law Impact Assessment (HUDERIA).

[3] Government of the Netherlands, FRAIA (Fundamental Rights and Algorithms Impact Assessment), more info online: https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms

[4] A Quintavalla, J Temperman (eds.), Artificial Intelligence and Human Rights (Oxford University Press 2023); J Fjeld, N Achten, H Hilligoss, AC Nagy, M Srikumar, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI* (January 15, 2020) Berkman Klein Center Research Publication No. 2020-1, DOI: http://dx.doi.org/10.2139/ssrn.3518482; A Kriebitz, C Lutge, 'Artificial Intelligence and Human Rights: A Business Ethical Assessment, in Business and Human Rights Journal' (2020) Vol. 5, Issue 1, pp. 84-104; G De Gregorio, 'From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society' (2019) in 11(2) *European Journal of Legal Studies,* pp. 65 ff.; C Fleissner, 'Inclusive Capitalism Based on Binary Economics and Positive International Human Rights in the Age of Artificial Intelligence' (2018) Vol. 17, Issue 1 Washington University Global Studies Law Review, pp. 201 ff.; F Raso, H Hilligoss, V Krishnamurthy, C Bavitz, K Levin Yerin, *Artificial Intelligence & Human Rights: Opportunities & Risks* (September 25, 2018) Berkman Klein Center Research Publication No. 2018-6, Available at http://dx.doi.org/10.2139/ssrn.3259344.

identification of a gap between the theoretical affirmation of a rule and its practical application. In fact, the AI Act alone is not sufficient to specify how to implement a FRIA effectively, because there are no indicated parameters for the implementation of adequate measurement paths. This need is starting to become increasingly clear in the literature[5].

2. Methodology.*

The methodology of the research is based on two phases: (i) the study of the existing legal and ethical frameworks concerning AI and human rights; and (ii) the translation of the identified rules and principles into a set of synthetic requirements to create an automated risk assessment prototype as output of the research.

The measurement approach by score has a profound impact on the civil system for the protection of harm to human beings and requires a revision of the traditional law methodologies as well as real changes at a regulatory level. The project has investigated in both directions: (i) the effective protection of human beings, and (ii) the rethinking of the regulatory methods in order to strengthen the *ex ante* evaluation models for AI. As a matter of fact, high-risk AI has legal relevance and can be involved itself in the decision-making processes related to the design and placing on the market of intelligent products.

The research is based on a multidisciplinary approach of interaction between humanities (law) and technical sciences (engineers). In fact, legals are able to identify the reference parameters of the research (in this specific case, fundamental rights to be analysed to verify the impact that AI has on them) as well as quantify the type and levels of violation for the purposes of measurement, to be evaluated according to a judgment of balancing opposing interests. Engineers, on the other hand, have the task of developing the prototype for measuring the impact of AI and automating it.

To better understand the effective protection of human beings in relation to AI systems and to define the proper parameters to be applied for AI risk assessment, the project will start with the analysis of the current legal framework.

3. State of the art.*

The state of the art on the legal and ethical regulation of AI is now quite complex. For further information, please refer to other ReCEPL studies on the topic[6]. In this paper, the focus is on the impact of AI on human rights.

---

[5] A Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template' (March 30, 2024), DOI: http://dx.doi.org/10.2139/ssrn.4782126.

[*] The authors of this paragraph is Dr. Maria Cristina Gaeta.

[*] The authors of this paragraph is Dr. Maria Cristina Gaeta.

[6] MC Gaeta, L Aulino, E Troisi E (2023), 'The possible relationships between law and ethics in the context of artificial intelligence regulation' (2023) 44 Humana.Mente Journal of Philosophical Studies, 44, pp. 163 ff.;

3.1 International and European existing legal and ethical framework concerning AI and human rights.

The state of the art concerning the impact of AI systems on human rights starts from the analysis of the International and European fundamental rights charters. Particularly relevant are the Charter of Fundamental Rights of the European Union (FREU) of 2000, the Universal Declaration of Human Rights (UDHR) of 1948 and the European Convention on Human Rights (ECHR) of 1950.

With specific regard to the judicial sector at the International Level, then, the European Ethics Charter on the Use of Artificial Intelligence in Justice Systems and their Environment (CEPEJ Charter) of 2018 should be taken as a point of reference. The CEPEJ Charter sets out five key principles that should be respected in the design and use of artificial intelligence (AI) by judicial professionals: (1) respect for fundamental rights, (2) non-discrimination, (3) quality and security, (4) transparency, impartiality and fairness, and (5) user control. After the CEPEJ Ethics Charter, of great relevance, is the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law of 2024, which formulates fundamental principles and rules to be respected within the lifecycle of AI systems to comply with certain fundamental principles: human dignity and individual autonomy, equality and non-discrimination, as well as, privacy and personal data protection.

Concerning the EU level, the most recent hard law regulation on AI is the AI Act, as part of a wider package of policy measures to support the development of trustworthy AI, which also includes the AI Innovation Package [7] and the Coordinated Plan on AI[8]. Together, these measures aim to guarantee the safety of AI technologies and the protection of the fundamental rights of individuals and businesses in relation to AI applications. They will also strengthen uptake, investment and innovation in AI across the EU. Also from an ethical point of view, the need to verify the impact of AI on individuals and on society in general [9] , as well as on society, human psychology, financial systems, environment and trust, has been highlighted in European studies[10] and soft law acts[11].

L Gatt L, IA Caggiano, MC Gaeta, L Aulino, E Troisi, 'The possible relationships between law and ethics applied to AI' (2023) 2 EJPLT, 111 ff., doi https://doi.org/10.57230/EJPLT232GCG.

[7] Communication from the European Commission on boosting startups and innovation in trustworthy artificial intelligence, 24 January 2024 COM(2024) 28 final, Official web page European Commission, AI innovation package to support Artificial Intelligence startups and SMEs, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383.

[8] Communication from the European Commission, Coordinated plan on Artificial Intelligence, 7 December 2018, COM(2018) 795 final, Official web page European Commission, Coordinated Plan on Artificial Intelligence, available at: https://digital-strategy.ec.europa.eu/en/policies/plan-ai.

[9] European Parliament Study, Artificial intelligence: From ethics to policy, PE641.507, June 2020

[10] European Parliament Study, The ethics of artificial intelligence: issues and initiatives, PE 634.452, March 2020; European Parliament Study, European framework on ethical aspects of artificial intelligence, robotics and related technologies, PE 654.179 – September 2020.

[11] European Parliament Resolution, Framework of ethical aspects of artificial intelligence, robotics and related technologies, of 20 October 2020, PROV(2020)0275; HLEG-AI, the Assessment List for Trustworthy Artificial Intelligence (ALTAI), 17 July 2020; European Commission White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, 19 February 2020, COM 2020/65 final; HLEG-AI, Policy and investment recommendation for trustworthy AI, June 26, 2019; Communication from the European

With specific reference to the methodology of the risk-based approach and, more specifically, the risk impact assessment, it seems appropriate to highlight that, in the last years, the EU approach has been based on the analysis of the impact of the risk of a product/service on human being's rights, from the design phase up to the introduction on the market and its related use. The first example is that represented by the Data Protection Impact Assessment - DPIA (Artt. 35-36 Reg. 2016/679/UE - GDPR), then also followed by the risk assessment on human rights arising from the design and operation of the very large online platforms and very large online search engines (Art. 34 Reg. 2022/2065/UE – DSA), with explicit reference also to fundamental rights (art. 34, para 1, lett. b)[12]. This risk analysis concretely implies a measurement of the risks on the basis of a given scale of values. It is therefore the evolution of the concept of measurement, also analysed from a legal point of view[13].

This is the context in which FRIA developed, expressly provided by the AI Act, for which certain high-risk AI systems shall be avalutated, at the preventive stage and monitored throughout thei entire lifecycle, throuth an assessment tool of the impact on fundamental rights that the use of such a system may produce[14].

3.2 Italian state of the art AI regulation, with specific reference to its impact on human rights.

At the Italian level, the state of the art starts from the analysis of the White Paper of the Agency for Digital Italy, entitled 'Artificial Intelligence at the service of citizens', published in 2018. In particular, challenge 8 was focused on measuring the impact of Artificial Intelligence solutions in public administration[15].

The White Paper approached the issue from two points of view: that of the citizens (quality of life of people and customer satisfaction) and that of the institutions (optimisation of organisational processes). The White paper underlines the need to assess the impact of AI technologies by applying a multidisciplinary approach to the measurement with the aim of designing and

Commission, Building Trust in Anthropocentric Artificial Intelligence, 8 April 2019, COM 2019/168 final; HLEG-AI, A definition on AI: Main capabilities and Disciplines, April 8, 2019; HLEG-AI, Ethical Guidelines for Trusted AI, April 8, 2019; Communication from the European Commission, Building Trust in Human Centric Artificial Intelligence, 8 April 2019, COM(2019) 168 final.

[12] A Mantelero, Putting the DSA into practice (Verfassungsbooks 2023), pp. 107 ff..

[13] L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI devices and their legal compliance: A prototype tool for its evaluation and measurement' (2022) 1 EJPLT 301 ff. DOI: https://doi.org/10.57230/EJPLT221LGIACMCGAAM.

[14] S Bertaina, I Biganzoli, R Desiante, D Fontanella, N Inverardi, IG Penco, A Cosentini, 'Fundamental Rights and Artificial Intelligence Impact Assessment: A New Quantitative Methodology in the Upcoming Era of Ai Act' (Jan 18, 2024), DOI: http://dx.doi.org/10.2139/ssrn.4698609; A Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI* (Springer 2022); H Janssen, Ah Lee MS, Singh J, 'Practical fundamental rights impact assessments' (2022) 30 International Journal of Law and Information Technology, pp. 200 ff., https://doi.org/10.1093/ijlit/eaac018; A Mantelero, SM Esposito, 'An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems' (2021) Computer Law & Securety Review, available at: https://doi.org/10.1016/j.clsr.2021.105561.

[15] White Paper of the Artificial Intelligence Task Force of the Agency for Digital Italy (AgID), 'Artificial Intelligence at the service of citizens', Version 1.0, March 2018, Challenge 8.

developing trustworthy AI, ensuring reliability and transparency as well as reducing the risk of errors (and therefore possible damages for the individuals).

In 2024, the concept of 'impact', albeit in a broader sense, is taken up, in AgID's Italian Strategy for Artificial Intelligence 2024-2026[16], with reference to scientific research, public administration, companies, and education. In particular, the need to enhance applied AI research emerges, through initiatives co-designed by public-private partnerships, focusing on contexts of greater economic and social value for Italy and with a greater impact on citizens' well-being. In addition, the strategy points out that public administration processes need to be made more efficient, with a specific focus on clearly delineated areas of intervention by the PA also considering the impact and risks of the AI systems.

Furthermore, in May 2024, the Italian Council of Ministers approved the Italian bill on AI, in line with the AI Act, which regulates the principles of research experimentation, development, adoption and application of AI systems, promoting their proper, transparent and responsible use, in an anthropocentric dimension, as well as ensuring supervision on economic and social risks and, specifically, on the impact of AI on fundamental rights (Art. 1). It also introduces principled rules and industry provisions to promote the use of new technologies for the improvement of citizens' living conditions and social cohesion, as well as to provide risk management solutions based on an anthropocentric view. The bill provisions intervene in five specific areas: national strategy, national authorities, promotion actions, copyright protection, and criminal sanctions.

4. Cyberjustice and FRIA: Integrating AI in Judicial Contexts.*

The implementation of a risk assessment model for AI systems aimed at ensuring effective protection of fundamental human rights necessitates a context-specific approach. The risk analysis methodology must identify the extent to which a high-risk system is likely to pose significant risks to human rights, especially considering the sectorial application context. When possible (or expressly required; cf. art. 27 AI Act), it should also take into account the specific deployment environment, the stakeholders likely to be affected, and their fundamental rights and freedoms actually exposed to risk from the system's use.

Our proposed model focuses on AI systems used in judicial and para-judicial (e.g., ADR/ODR) contexts for the resolution of legal issues. The risk assessment of AI must be contextualised to the specific area of use, which involves analysing the unique risks to fundamental rights associated with the intended use of AI systems in judicial contexts. The area of cyberjustice indeed presents a unique set of challenges and risks for the use of AI. These systems are not only subject to the AI Act (at least to the extent that they can be defined as high-risk), but also operate within a multi-level domain-specific regulatory framework. This framework includes supranational regulations, such as the

[16] Agency for Digital Italy (AgID), 'Italian Strategy for Artificial Intelligence 2024-2026', April 2024, pp. 3-7.
* The authors of this paragraph is Dr. Emiliano Troisi.

recent Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024), and guidelines like the CEPEJ European Ethical Charter on the use of artificial intelligence in judicial systems and their environment (2018) and the related Assessment tool for the operationalization of the Ethical Charter (2023). Additionally, national rules often regulate how to implement or use AI in the justice sector in compliance with fundamental rights obligations (e.g., in Italy, the Bill providing for delegation to the government on Artificial Intelligence, 2024, currently under parliamentary discussion).

This comprehensive framework contributes to defining the limits and compliance requirements for cyberjustice systems and needs to be carefully considered, alongside the broader human rights framework and the current state of the art on ethical AI, in order to contextualise and detail the identification and evaluation of both the specific threats to fundamental rights that AI systems pose in the given context of application and deployment, and the appropriate measures for the overall mitigation and control of these risks.

Establishing an AI FRIA assessment tool that is specific to the judicial domain is indeed crucial for ensuring effective ex ante evaluation and iteractive governance of cyberjustice systems in a way that is relevant under the AI Act and in any case ensures proper assessments of AI systems helping to avoid unexpected or unwanted harms. Furthermore, it can also be used as a benchmark for conceptualising and defining specifications for the design of AI systems in the judicial domain.

5. Objectives.*

The main objective of the project is the identification of parameters for AI risk analysis and the creation of metrics for each parameter for the concrete measurement of AI risks for individuals. This main objective is a result of the application of the following procedural steps:

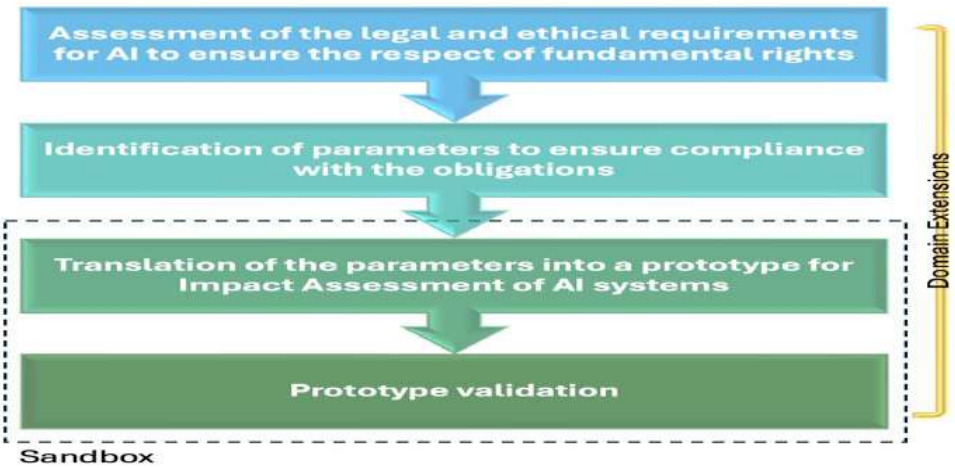


Image no. 1 – Objectives of the research

* The authors of this paragraph are Dr. Roberto Trasarti, Dr. Roberta Savella and Dr. Francesca Pratesi.

To reach this main objective, the output of the research consists in the design of tool prototype to support and automate the fundamental rights impact assessment of high-risk AI systems, in line with the requirements of the AI Act, i.e. an automated implementation model of the FRIA (Fundamental Rights Impact Assessment), required by the European AI Law, that has these characteristics.

6. The analytical process. *

The implementation model of the FRIA will be developed in the form of a semi-automatic prototype specifically designed for this purpose. The design phase of the project will focus on AI systems used in the administration of justice, as a relevant area of application of high-risk systems for which the AI Act requires deployers to perform a FRIA.

The research activity in this part of the project will start with two parallel assessments: (i) the selection of a list of fundamental rights, as described in the relevant European and International Charters, that are mostly impacted by the use of AI systems in the judicial sector; and (ii) the identification of the components of an hypothetical AI system used in this sector – for example, the training data, the algorithm, and the interface.

Following said assessments, the research team will single out a series of parameters and attributes that influence the impact of the AI systems used in the judicial field on fundamental rights and will translate them into machine-readable keywords. For example, one attribute that is very likely to have a significant impact on the fundamental right to equality and, in particular, non - discrimination, before the law is ethnicity (very often referred to as 'race' in the literature and legal documents), as we have seen in the debate surrounding the use of the software 'COMPAS'[17]. Therefore, there will likely be the need to include 'ethnicity' as a keyword for the prototype to analyse in its impact assessment on equality and non-discrimination. Moreover, it is important to also consider the proxy parameters that can be associated with the attributes identified. For example, numerous studies have concluded that the zip code is very often a proxy for 'ethnicity'[18].

Therefore, the first step of project will be the identification of the fundamental rights that are primarily relevant when applying AI systems in the justice sector, in order to ensure their protection. We considered three sources as starting point: the charter of Fundamental Rights of the European Union, the Universal Declaration of Human Rights and the European Convention on Human Rights, obtaining the following preliminary selection of fundamental rights that can be related to the judicial field.

---

* The authors of this paragraph are Dr. Roberto Trasarti, Dr. Roberta Savella and Dr. Francesca Pratesi, with the contribution of Dr. Maria Cristina Gaeta.

[17] J Angwin, J Larson, S Mattu, L Kirchner, 'Machine bias' (2016, 23 May) ProPublica' https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; A Lee, 'Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing' (2019, 19 February) UCLA Law Review, https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/.

[18] M Favaretto, E De Clercq, BS Elger, 'Big Data and discrimination: perils, promises and solutions. A systematic review' (2019) 12(6) J Big Data https://doi.org/10.1186/s40537-019-0177-4.

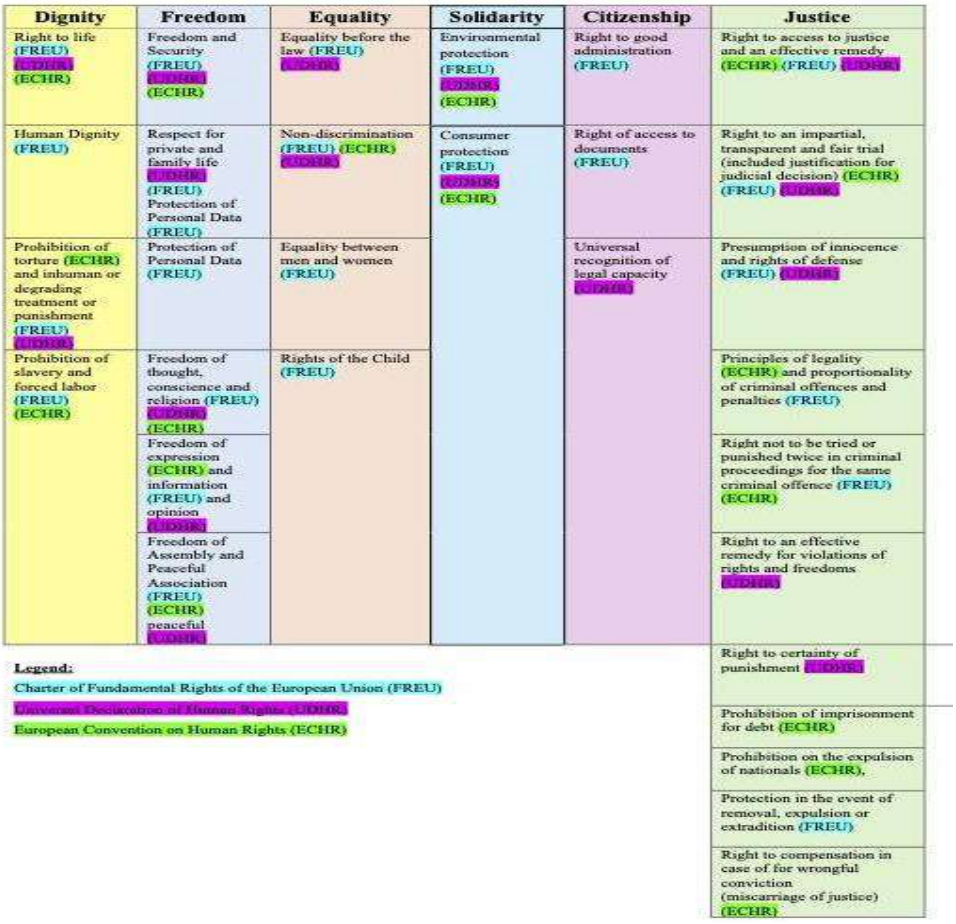


Image no. 2 – First selection of fundamental rights in the judicial filed

From this first set we want to identify specific protected attributes by examining the relevant laws (as shown in the example we provide in the next section) and therefore specific algorithms to extract quantifiable metrics which are relevant to evaluate the impact of the AI system on fundamental rights.

The second step of the experiment will be the planning and implementation of an empirical legal study (ELS) based on the impact of AI applications in the judicial field in concrete. It will then be necessary to play out concrete scenarios of using an AI system to test its operation. In this light testing environments of high-risk AI systems are of great importance, also in light of the AI Act provisions. More precisely, testing in real-world conditions outside AI regulatory sandboxes (art. 60-61 AI Act), as well as, more in general, testing activities in compliance with art. 9 AI Act, can guarantee simulations of operational environments in which to test the functioning of selected domains of high risk AI systems to complete the assessment. Indeed, experimentation through testing in real-world environments and sendboxes allows a way out of self-assessment, thus avoiding the problems in which all current evaluation systems (e.g., ALTAI or HUDERIA) are locked. In the testing phase, indeed, there will be the need to analyse each component of the theoretical AI system: the data used for training the algorithms, the model extracted and the output

obtained by the application of the model on new data, the functioning of the AI system.

The third step of development will be the elaboration of metrics for each parameter for the concrete measurement of AI risks for the individuals. THe metrics will also be created through the individuation of algorithms to extract these metrics for assessing the impact of AI on the selected fundamental rights.

Finally, the fourth step will be the concrete and automatic measurement of the impact of AI on the selected parameters, using the individuated metrics (automatic evaluation of the results of the experiment). The team will then design a translation matrix that will use the outputs of the abovementioned steps, translating them into specific keywords to automatically assess the impact of the individual AI system on the fundamental rights previously selected. This operation will provide quantifiable metrics that will be used to calculate the overall impact on the fundamental rights of the AI system analysed.

7. Experiment design.

In order to show the approach, we present how we are addressing the problem in the case of equality and, more specifically, focusing on the right to non-discrimination.

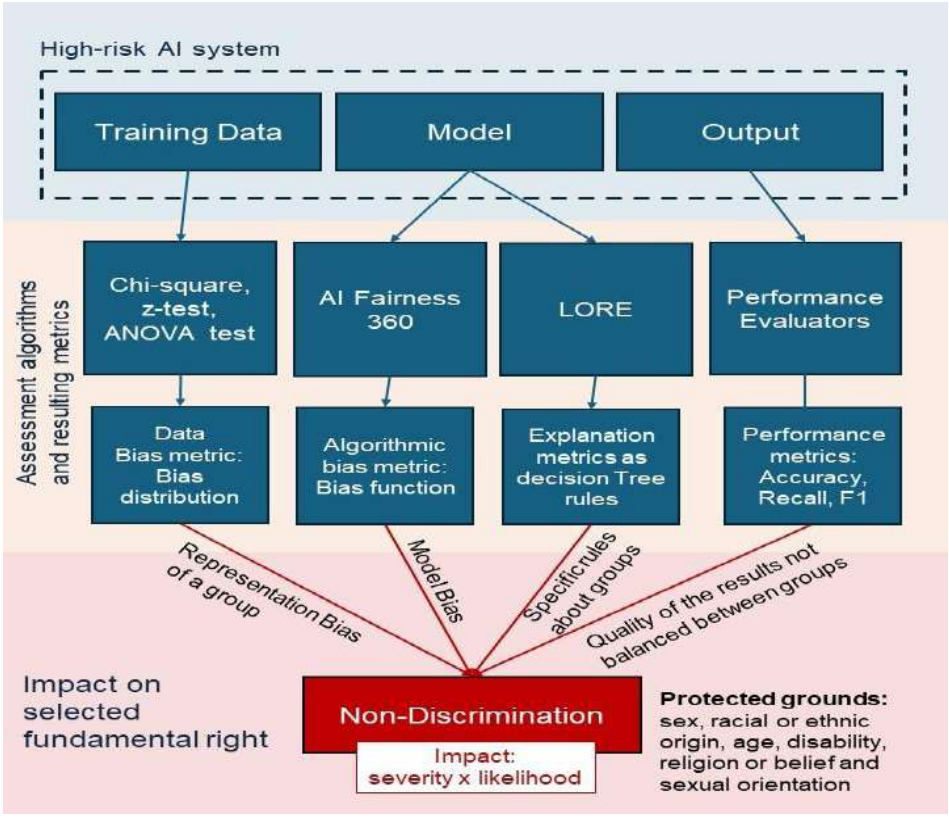


Image no. 3 –Assessment algorithms and resulting metrics for measuring the impact of high-risk AI on non-discrimination right.

We selected this right as literature has observed the discriminatory effects of biased systems[19] and it is particularly relevant for the use of AI in the judicial field, as shown by the COMPAS case[20]. Moreover, we believe that the selection of keywords in this context can be facilitated by the fact that European non-discrimination law prohibits differential treatment on the basis of a fixed and limited list of "protected grounds" i.e. "*characteristics of an individual that should not be considered relevant to the differential treatment or enjoyment of a particular benefit*"[21]. The protected grounds addressed by the European non-discrimination Directives are: sex, racial or ethnic origin, age, disability, religion or belief, sexual orientation. To design our prototype, we can use these protected grounds as keywords and for each keyword we will identify quantifiable metrics to be measured with automated tools integrated in our prototype. For the purpose of this example, we selected the 'ethnicity' attribute, as it was particularly relevant in the COMPAS case[22]. We theorised a system composed by training data, model and output. To examine this system, we would need to apply algorithms for three purposes: bias detection and fairness auditing, explainability, and evaluation of the performance. To analyse the dataset, we could integrate in our model some statistical methods used in this field, like Chi-square, Z-test, and ANOVA test, to assess the bias distribution in the training data[23]. For bias detection in the model, we identified the open-source toolkit AI Fairness 360 [24] that could be integrated into our model through its publicly available APIs. This tool would identify representation biases in the system, allowing our prototype to calculate the impact on the right to non-discrimination. To obtain the explainability of the system we could apply LORE[25] or other existing explainable AI algorithms[26]. LORE is an agnostic method used to provide interpretable and faithful explanations for black box systems, and we could use it to find out the specific rules applied to the different ethnic groups. Specific metrics we would analyse for explainability are fidelity, faithfulness, completeness, comprehensibility, succinctness, and stability. Finally, we would need to apply a statistical evaluator to determine the accuracy, recall and F1 of the output, so we could evaluate whether the quality of the result is balanced or not balanced among the different ethnic groups.

---

[19] J Buolamwini, T Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.
[20] J Angwin, J Larson, S Mattu, L Kirchner, 'Machine bias' (2016, 23 May) ProPublica' https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[21] European Union Agency For Fundamental Rights, "Handbook on European non-discrimination law – 2018 edition", February 2018, https://fra.europa.eu/en/publication/2018/handbook-european-non-discrimination-law-2018-edition.
[22] J Angwin, J Larson, S Mattu, L Kirchner, 'Machine bias' (2016, 23 May) ProPublica' https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[23] ER Girden (1992). ANOVA: Repeated measures. Sage Publications, Inc.
[24] N Mehrabi, F Morstatter, N Saxena, K Lerman, A Galstyan, "A Survey on Bias and Fairness in Machine Learning", arXiv:1908.09635v3 [cs.LG]
[25] R Guidotti, A Monreale, S Ruggieri, D Pedreschi, F Turini, F Giannotti, "Local Rule-Based Explanations of Black Box Decision Systems", arXiv:1805.10820v1 [cs.AI]
[26] D Rudresh, D Devam, N Het, S Smiti, O Rana, P Pankesh, Q Bin, W Zhenyu, S Tejal, M Graham, R Rajiv 'Explainable AI (XAI): Core Ideas, Techniques, and Solutions' (2023) 55(9) ACM Comput. Surv, Article 194 https://doi.org/10.1145/3561048.

8. Conclusions.

Both at the international and European levels, there is a clear understanding of the need to protect human beings from specific processes and products endowed with high-risk AI systems, and the need for such protection to be carried out to prevent damages, thus generating an AI assessment with regard to the fundamental rights as outlined in the relevant 'constitutional charters' of the EU and international framework. What is lacking is an effective risk assessment tool for deployers of high-risk AI systems. In this light, the study proposes a concrete FRIA implementation model, in line with the AI Act. Indeed, FRIA is envisaged in the European AI Act but, not specified in its structure nor in its implementation methodologies, and this is because the FRIA approach generates, from a legal point of view, conceptual and normative issues that affect the current system of the protection of human rights by autonomous agents.

Kostenko OV, Ghaziani VA, 'Admissibility of illegally obtained e-evidence: A critical study of EU law and the precedents of the European Court of Human Rights' (2024) 2 EJPLT, 205 – 220.
DOI: https://doi.org/10.57230/EJPLT242OVKVAG

EJPLT
ISSN 2704-8012



Admissibility of illegally obtained e-evidence: A critical study of EU law and the precedents of the European Court of Human Rights

Ammissibilità delle prove elettroniche ottenute illegalmente: uno studio critico del diritto dell'UE e dei precedenti della Corte europea dei diritti dell'uomo

OLEKSII VOLODYMYROVYCH KOSTENKO
Associate Professor
Faculty of Law of the National Aviation University

VAHID AKEFI GHAZIANI
Pre-doctoral candidate
International University College of Turin
Attorney at law
Central Bar Association of Iran

Abstract

Whether illegally obtained evidence should be deemed inadmissible is a question that many jurisdictions still struggle with. In this regard, there is no internationally accepted standard that orients national jurisdictions in detaching valid from invalid evidence. This study focuses on the two-fold legal systems practiced within EU law and that of the European Court of Human Rights in order to identify their points of disagreement and to approximate the two systems. The outcomes suggest that the GDPR has not provided any balancing guidance for inconsistent fundamental rights; therefore, EU member states have wide discretion in prevailing one right over another. Despite this, aiming to protect EU fundamental rights, particularly the right to protection of personal data (Article 8 of the EU Charter) and the fairness procedure of a trial (Article 47 of the Charter), national courts, in the absence of domestic guidelines, are welcomed and urged to follow the ten-factor test of the judgment Beuze v. Belgium (ECHR, November 8, 2018). Finally, after examining the court's guidance, the paper at hand partially changes the test and offers a more reliable test to reconcile privacy rights with the right to a fair trial. This test could serve as a yardstick for national courts as well as upcoming ECtHR precedent.

© The author(s) 2024, 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
Se le prove ottenute illegalmente debbano essere considerate inammissibili è una questione con cui molte giurisdizioni ancora lottano. Non esiste un criterio riconosciuto a livello internazionale che orienti le giurisdizioni nazionali a tal riguardo. Questo studio si concentra sui due sistemi giuridici esistenti nel diritto dell'UE e in quello della Corte europea dei diritti dell'uomo al fine di identificare i punti di disaccordo e di avvicinare i due sistemi. I risultati suggeriscono che il GDPR non ha fornito alcuna guida per bilanciare i diritti fondamentali incoerenti; pertanto, gli Stati membri dell'UE hanno un'ampia discrezionalità nel far prevalere un diritto rispetto a un altro. Nonostante ciò, al fine di tutelare i diritti fondamentali dell'UE, in particolare il diritto alla protezione dei dati personali (articolo 8 della Carta UE) e l'equità del processo (articolo 47 della Carta), i giudici nazionali, in assenza di orientamenti nazionali, hanno accolto favorevolmente e sono sollecitati a seguire il test dei dieci fattori della sentenza Beuze c. Belgio (CEDU, 8 novembre 2018). Infine, dopo aver esaminato le indicazioni della Corte, il documento modifica parzialmente il test e offre un test più affidabile per conciliare i diritti alla privacy con il diritto a un processo equo. Detto test potrebbe servire da metro di paragone per i tribunali nazionali e per l'imminente precedente della Corte EDU.

Keywords: Admissibility of electronic evidence; European Court of Human Rights; EU Law; Fair trial; Fundamental rights; Right to privacy

Summary: Introduction. – 1. Legal sources. – 1.1. EU Legislations. – 1.2. Defensible argument. – 2. Precedents of the ECtHR. – 2.1. Discourse about the role of e-evidence. – 2.2. What has been done so far? – 2.3. Defensible argument. – Conclusion.

Introduction.

Beyond any doubt, the probative value of evidence plays a game-changing role in trial procedures. However, over time, as electronic evidence has gained similar value to old forms of evidence, traditional standards of proof have been exposed to significant changes.[1] Besides, the development of new technology, tech-friendly legal approaches,[2] and the hardships usually involved in gathering physical evidence have all eased and spurred the presentation of e-evidence in judicial procedures.[3]

[1] One major distinguishing feature of digital evidence is its authenticity. Democratic societies have often laid down lengthy and in-depth guidelines for digital forensics with respect to different stages, including pre-lab investigations and prior as well as post-trial stages. For instance, see Association of Chief Police Officers, *ACPO Good Practice Guide* (Cm version 5.0, 2012) section 2. Also see relevant attempts by the European Union in: Council of Europe, 'iPROCEEDS-2: Launching of the Electronic Evidence Guide v.3.0' (Council of Europe, 22-23 June 2022) <https://www.coe.int/en/web/cybercrime/-/iproceeds-2-launching-of-the-electronic-evidence-guide-v-3-0> accessed 21 May 2024.

[2] For instance, through the Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market [2014] OJ L 257/73, the admissibility of electronic signatures (Art. 25), electronic seals (Art. 35), electronic time stamps (Art. 41), and electronic documents (Art. 46) have been ensured and proposed for the national electronic identification scheme throughout EU member states (see P. 9 of the said Regulation).

[3] National lawmakers are not the sole actors facilitating and ensuring the e-evidence exhibition; cross-border powers likewise do the same; as an example, see European Parliament and Council Regulation (EU) 1543/2023 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal

Moreover, national jurisdictions have different viewpoints in regard to the admissibility of illegally obtained evidence,[4] which has sparked a lot of concern among scholars in order to harmonize national jurisdictions in the paradigm of mutual admissibility. [5] Nevertheless, the idea of borderless obtaining of evidence and cross-border admissibility, however impressive it sounds, embraces various problems due to the dissimilar domestic frameworks.[6]

Such evidences simultaneously carry out two attributions: first, they form the facts of the case, and second, they indicate that the undergone investigatory procedure contained some illegal elements that led to a breach of a legal provision.[7] Whether courts should accept illegally obtained evidence will make an extensive difference; not only might the outcome of a dispute be subjected to a substantial change, but also the admission of such evidence will further impact the democratic values within a society. This paper examines the admissibility issue of e-evidence, where the evidence is gathered through infringing the right to the protection of personal data.[8] However, the paper has taken a legal-dogmatic methodology and therefore does not address interdisciplinary analyses. Meanwhile, concerning the approach, this survey attempts to develop an approximate matching point for two closely related but

proceedings [2023] OJ L191/118 p. 2 and 4. This regulation has set out the framework for preserving and production of e-evidence across the Europe. Another example is the Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters [2014] OJ L130/1, see specifically Article 9 which ensures the without delay execution of European Investigation Orders (EIO). However, this paper does not address the judicial procedures in cross-border paradigm.

[4] K Ligeti, B Garamvölgyi, A Ondrejová, and M von Galen, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 eucrim, 203 <https://eucrim.eu/media/issue/pdf/eucrim_issue_2020-03.pdf> accessed 6 June 2024. However, when it comes to the admissibility issue, it is indispensable to designate the grounds on which electronic evidence is deemed admissible or inadmissible. Regardless of the illegal methods through which evidence is obtained, there are often several grounds in different systems that constitute a basis for rendering e-evidence inadmissible. Depending on how we define admissibility and authenticity, the justification for which e-evidence would be suppressed differs. For instance, in *Lorraine v. Markel American Ins. Co.* 241 F.R.D. 534 (D. Md. 2007) at para 542. The judgment classified 'authenticity' as a category under 'admissibility' of e-evidence. However, we think the two concepts should have different meanings and scopes of application. The authenticity of e-evidence refers to a situation where there is a link between afforded evidence and an actor (ex., a wrongdoer or claimant). In the absence of such a link, the contested evidence shall not be attributed to the accused and is therefore invalid (not inadmissible). To see advocates of this proposal, turn to C Reed, 'The admissibility and authentication of computer evidence - a confusion of issues' (1990) 6 CLSR 13. Seemingly, the same advocacy could be seen in C Singh, *Unlocking the law of evidence* (4th edn, Routledge Publishing 2023) 17 (Questions of admissibility are questions of law.) On the contrary, section 28 U.S.C. § 1731 and the mentioned judgment in *Lorraine v. Markel* seem to have adopted a wider conceptual domain for 'admissibility.'

[5] M Kusak, 'Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters' (2017) 23 Eur J Crim Policy Res, 337. Recently, European Law Institute has published a draft proposal on the matter as well, see C Wendehorst (Director), *'ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings'* (Draft Legislative Proposal of the European Law Institute, European Law Institute 2023), in Article 2 (scope).

[6] M Corhay, 'Private Life, Personal Data Protection and the Role of Service Providers: the EU E-Evidence Proposal' (2021) 6 European Papers, 441, 444.

[7] Legal duties or rights, and manifestly fundamental rights, might be the subjects of a breach. However, minor breaches are mostly overlooked by legal systems. These types of violations usually do not form a situation in which a judge should consider their dismissal or approval of admissible and authentic evidence. This idea of ignoring minor breaches has also been reflected in the well-known maxim '*De minimis non curat lex*' which translates to 'trifles are not the matter of the law's consideration.' See, BA Garner, *Black's Law Dictionary* (9th edn, Thomson Reuters 2009) 496.

[8] Article 8 of the EU Charter of Fundamental Rights (Protection of personal data) and Article 8 of The European Convention on Human Rights (Right to respect for private and family life).

different legal systems: The European Union and the European Court of Human Rights. (ECtHR).[9]

Nevertheless, since the market for sensitive data is astonishingly influencing the data economy[10] and correspondingly gaining intense consideration in scholarly debates and academic research,[11] the paper also examines evidence related to sensitive information to better organize its context.[12] The trajectory of the present paper could be sketched out as follows: The first part examines the current legal framework of the EU in response to the illegitimate obtaining of e-evidence. Cross-border disputes, such as those initiated with the issuance of EU warrants and the EU itself, are entirely outside the scope of our argument.[13] Conversely, part one clarifies the perspective of the EU's legal instruments, including the General Data Protection Regulation (2016). This part, along with exploring GPRS' relevant provisions on the admissibility issue, argues that the topic has fallen beyond the interest sphere of the EU's legislative. In other words, this part clarifies two issues: 1. Has the EU touched upon domestic procedures in any manner that serves member states in determining the admissibility of ill-founded evidence? 2. To what extent is the EU's legal framework capable of balancing different conflicting fundamental rights (namely, data protection on one side and other fundamental rights on the other)? This part also considers an argument about sensitive data (Article 9 GDPR), since it may shed light on the status of non-sensitive personal data. Consequently, the second part discusses the approach of the European Court of Human Rights' approach in terms of the admissibility issue. In this part, two questions have been raised and answered: 1. What is the perspective of the

[9] Although the two distinct systems stem from dissimilar treaties, they relatively hold a close connection in our argument since Articles 6 and 13 of the Convention are reaffirmed by Article 47 of the EU Charter. See, the Judgment of 27 Februrary 2018, Associação Sindical dos Juízes Portugueses v. Tribunal de Contas, C-64/16, EU:C:2018:117, paragraph 35.

[10] Namely, health data (as classified under Article 9(1) GDPR) has seen glaring economic growth over recent years. It is noteworthy that, while the worldwide market for digital health reached 45.69 billion dollars in 2017 and 170.25 billion dollars in 2023, it is estimated to peak at 274.93 billion dollars by 2028. See Statista Market Insight, 'Digital Health – worldwide' (Statista, Updated February 2024) <https://www.statista.com/outlook/hmo/digital-health/worldwide> accessed 21 May 2024.

[11] In addition to economic value, many research studies also address ethical issues of the case. For instance, considering the de-identification of personal data through available or publicized information has led some authors to propose the idea of prioritizing regulatory attempts on the public flow of data rather than private shares. Therefore, if a website faces normative restrictions on publicizing personal information, the tactics of hackers and infringers (which are similar to reverse engineering methods) would probably reach a dead end. See, P Ohm, 'Broken promises of privacy: Responding to the surprising failure of anonymization' (2010) 57 UCLA LR 1701, 1776.

[12] Vividly, whenever a legal instrument addresses one of the two categories of data (sensitive or non-sensitive personal data) due to their shared features of being, firstly, 'data' and secondly, 'personal data,' which are not yet publicized, it tacitly addresses the other category. For instance, in light of the provisions of GDPR, one could benefit from both Art. 6 and 9 when they are normalizing a share feature. This is due to the fact that the tenors of specific provisions (or, let's say, propositions in general) are often enlightened through the context of the general ones. Canon principle of 'Ejusdem generis' namely remarks how the sequence of general and specific should be used in interpreting the text of law. See related judgments in G A Dietz, 'Statutory Construction: Ejusdem Generis Versus Legislative Intent' (1950) 3 Fla. LR 258. At the time of writing this paper, the famous case (of *Fischer v. United States* (Docket No. 23-5572)) related to the U.S. Capitol attack of 6 January 2021 is pending in the Supreme Court of the United States. The case, however, deals with the interpretation of section 18 U.S. Code § 1512(c)(2) regarding obstructing official proceedings and one of the centralized arguments in the case touches on the role of Ejusdem maxim in the interpretation of the article; see, for example, pp. 13–15 of the filed response of petitioner 'J. Fischer' (filed on 28 March 2024) in the case.

[13] See, n 2 and 3.

ECtHR in confronting claims where the evidence of a dispute was obtained in such a manner that undermines the Article 8 of the European Convention on Human Rights (hereinafter, the Convention)? 2. Despite what the court has done so far, should the court's practical guidelines be altered or replaced by a new instruction in order to protect the effectiveness and objectives of the Convention?

Finally, It should be pointed out here that the current paper delimits its scope to precedents of the ECtHR[14] and EU law. Undoubtedly, the procedures of the CJEU will contribute to the interpretation of the GDPR. Therefore, the basis of the old case laws of the court related to Directive 95/46/EC will gradually phase out and be substituted by new perspectives outlined in GDPR (2016).[15] Likewise, the decisions of the ECtHR have the same role. Furthermore, since there are numerous grounds for evidence to be rendered inadmissible, except the one that deals with inadmissibility given to individuals' privacy infringement, other grounds are not considered in this paper.

1. Legal Sources.

1.1. EU Legislations.

Incident response, which is often conducted by parties to a case or their agents[16], digital forensics, and typical legal discoveries could all be involved before presenting digital evidence at trial. Courts, however, by being cautious about admitting this evidence, have highlighted the pivotal role of e-evidence in judicial hearings. [17] Nevertheless, no unique standard has so far been introduced by the EU lawmaker in harmonizing domestic judicial procedures or the EU's internal judicial order. [18] Whereas the EU Charter grants discretion to

[14] Since the protection of individuals' privacy falls within the scope of the EU Charter (Articles 7 and 8), the Court of Justice also has the authority to practice its competence in order to judicially preserve the said right. In doing so, an action for annulment (according to Art. 263 of the Treaty on the Functioning of the European Union) or either a preliminary reference by a national court (Art. 267 TFEU) are the two routes through which the court decides on the mentioned issue. Take as an example the recent case of the Court, wherein the Court, in response to the preliminary reference by the Brussels Court of Appeal, recognized TC String (transparency and consent string) as personal data under Art. 4(1) of the GDPR if there is a reasonable likelihood of re-identification (in the phrasing of the Court, the criterion is 'reasonable means'). See Judgement of 7 March 2024, *IAB Europe,* C-604/22, EU:C:2024:214, paragraph 43. For action of annulment, turn to the Order of the General Court on 7 December 2022, *WhatsApp Ireland Ltd v EDPB*, T-709/21, EU: T:2022:783, paragraphs 15 and 16.

[15] A Guzewicz, 'Uniform interpretation of General Data Protection Regulation concepts as a new challenge for CJEU' (2020) special Issue EJPLT, p. 8.

[16] Cyber engineers, for ensuring the organisation's network, take into account all the present or forthcoming incidents that may threaten its security. A Zamfiroiu and R C Sharma, 'Cybersecurity Management for Incident Response' (2022) 4 RCSJ 69, 69-75. Therefore, digital evidence of a crime might be gathered through this route.

[17] For instance, see *State v. Acosta* 311 App. 136, 489 P.3d (Or 2021) at para 608; *Commonwealth v. Carrasquillo* 13122 (Mass 2022). Both cases directly addressed the admissibility issues of evidence arising from sharing incriminating posts on social media. Also see the judgement in *Commonwealth v. Yusuf* 488, 379 (Mass 2021).

[18] While in recent years the issue has captured the EU's attention, the endeavours culminated in proposal 2018/0108 (European Production and Preservation Proposal) and ended up with the Regulation of 2023/1543, which sought to harmonize the existing context of obtaining e-evidence across borders. Regardless of this commendable move, the current legacy for diagnosing data safety within undertakings of national jurisdictions can be found in the provisions of the General Data Protection Regulation and the e-

the member states to codify effective regulations in compliance with EU fundamental rights, this, at first glance, justifies the silence of EU legislators in the case. Article 15 of Directive 2002/58/EC (ePrivacy) mandates member states to enact proportionate legislative measures to protect against the unauthorized use of electronic communications or activities that pose a risk of breaching the confidentiality of e-communications (as provided in Art. 5).[19] The general principles of the GDPR, on the other hand, reflect a clear-cut outlook for minimizing the risks of unlawful data processing. For instance, Article 5(1)(c) [20] and Art. 25 (Privacy by design and by default) have laid the groundwork for optimized methods of de-identifying, which must be followed by member states' domestic laws. [21]

However, a subtle inconsistency between the objectives [22] and other provisions of the GDPR could be observed.[23] GDPR allows holders of sensitive data, for instance, healthcare centers, to freely exchange patients' data; under the circumstances of Article 9(2)(f) processing of special categories of data (sensitive personal data) is not prohibited. The paragraph reads:

'processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity'

Privacy Directive. Frustratingly, given the tenor of Art. 15(1) of the European e-privacy directive, member states may approve legal guidelines for preventing illegal disclosure of personal data, such as interception of communication (Art. 5, e-privacy), but the directive per se has not provided detailed consideration about the admissibility of e-evidence.

[19] Since the evaluation of evidence, introducing standards of proof, and the allocation of *onus probandi* often mingle with the domestic sense and traditional legal customs of each member state, this might justify the lack of intervention from the EU. Also, the relevant competences of the EU should be considered. Whether regulating the current issue falls within the competencies alluded to in the Treaty on the Functioning of the European Union (TFEU), notably Articles 3 and 4, which have addressed the exclusive and shared competences of the EU, is also a crucial matter in need of solution.

[20] Principle of Data Minimisation.

[21] The exact method for de-identification, such as anonymization or pseudonymization, has not yet been established through EU law. In terms of sensitive data, specifically health data, Art. 44(2)(3) of the proposal for European Health Data Space (2022/0140 (COD)) signaled both anonymization and pseudonymisation as safe methods under the principle of data minimisation. Even with this clarification, the acceptable techniques of anonymization and pseudonymization still suffer from a lack of certainty, which makes health service centers and, in general, holders of sensitive data hesitant to employ legitimate techniques.

[22] See, Article 1 (2) GDPR and Recital 4.

[23] However, not to mention that governments also tend to accept illegal evidence, even if it is obtained through an illegitimate route. They might justify this policy with countless arguments. Mostly, such excuses try to overweight public interest or much more convoluted notions such as national security. However, in the digital era and in the context of sensitive data, the policy of 'ends justifies means' should be interpreted narrowly. Several reasoned explanations are capable of reinforcing the proposition. First and foremost, the abstract concepts of public interest or security are extremely flexible. They are prone to being easily abused or misused by their supplicants; whatever they plead for, they can simply interpret such concepts in their own favor. Second, the proliferation of digital means and the rapid reliance of society on digital areas have given rise to high expectations among users and are transforming the present form of life. In the meantime, in accordance with social needs and expectations, the law should be tasked with organizing an intense volume of human behavior in terms of legality and accountability. Moreover, in any case where illegitimate evidence finds its way to the tribunal, there will always be numerous negative consequences: 1. The exhibition of ill-founded evidence, even if suppressed by the court, leaves its traces on judge's bias and state of mind, which directly target the impartiality of judges. However, since there is no palpable deviation of the court from the rule of law, there would be a minor chance for the defendant to successfully challenge a biased decision in these circumstances. 2: The judgment allowing such evidence opens the floodgate to many other allegations and disputes. It may also pave the way for frivolous claims as well as dilatory tactics by parties. 3: The judgments trying to balance 'right to a fair trial' or 'public interest 'and 'protection of data' intensively influence the interpretation of the aforementioned concepts. The court's interpretation methodology, even if mistakenly applied in a specific case, potently inspires future judgments, the legal framework of the nation, and scholarly debates.

GDPR has not only left the issue of admissibility unresolved but also, given the general tenor of Article 9(2)(f), has offered a conservative and broad leeway for member states. The four grounds of necessity, as marked out in this paper, allow national courts to arbitrarily apply the law. Should the warrantless prosecutorial interrogations, police interrogations or even an inquiry from a potential claimant fall in the domain of 'establishment' or 'exercise,' it would have a game-changing role in legal procedures. However, Article 10 demystifies the procedure that is legitimate for gathering incriminating data. Here we are not arguing that the essence of 'data protection' entails banning warrantless access to sensitive data, which both Article 10 of GDPR and the Law Enforcement Directive (2016)[24] emphasize, but the sole suggestion is that warrantless access or any other type of illegitimate evidence gathering should not divert courts from assessing the admissibility of afforded evidence in their decision-making process. In other words, the GDPR does not balance the contradictory battle of fundamental rights;[25] rather, it hands over the task of weighing two or more inconsistent rights to national courts. Therefore, if an inquiry into a hospital has been made by an interrogator, government officer, or individual who has asked the data holder for the personal information of a patient, the court should assess the validity of the evidence with respect to GDPR. This is because the GDPR does not aim to balance two conflicting fundamental rights, and its provisions attempt to protect personal data in a pre-dispute area with an inhibitory approach.[26]

However, if an objection raises and alleges that GDPR provided by Recitals 1, 2, and 4 considers a potential clash of different fundamental rights, such as the right to a fair trial as pointed out in Recital 4, we dispute this argument by three major points:

1. Recital 4 calls for three conditions in order to strike a balance between 'protection of personal data' and other fundamental rights: a) This right should not be considered an absolute right; b) It should be perceived with respect to its societal functions. c) The balance between its peer fundamental rights should be stuck in accordance with the principle of proportionality. Consequently, the Recital tips off what the regulation has

[24] Article 10 of the Directive (EU) 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 [2016] OJ L 11/89.

[25] For instance, if privacy, freedom of speech, or the right to a fair trial contradict each other, no reasoned measurements have been taken by the Regulation.

[26] The main goal of GDPR is to leave behind a deterrent effect. Hence, provisions imposing rigid requirements of opt-in consent (e.g., Art. 7 and Recital 32), severe sanctions (e.g., Art. 83), and uncompromising obligations on the part of data holders (e.g., Art. 24, 25, and 31), all together with the asymmetrical distribution of rights and duties among data subjects and data holders (see GDPR, Chapter 3, Arts. 12–23), convey an overemphasis on the inhibitory approach of its nature. Albeit, the objectives of GDPR as set out in Article 1 are twofold: 1) protecting fundamental rights; and 2) free flow of personal data. See General Secretariat of the Council 14994/1/19 REV 1 of Council's position and findings on the application of the General Data Protection Regulation (GDPR) [2020] JAI 1312, paragraph 1); However, the provisions of GDPR lack an all-inclusive balancing between different fundamental rights, examining relevant rights and duties in court procedure, a profound examination of moral damages with delimitation of their applicatory scope (Art. 82), and frustratingly, a lack of any provision in regard to allocating administrative fines (in particular whether or not the lack of negligence would completely eliminate or diminish the amount to a trivial sum).

done so far with these words: 'This regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter.' However, this enigmatic silence right after addressing the three requirements of balancing, which baffles every reader in the latter two phases (societal function and accordance with the proportionality rule), should be considered a clue that singles out the imbalance approach of GDPR's measurement. [27]

2. The convoluted process of balancing two or more fundamental rights is fettered by a deep analysis of the different matrixes of each case and is a time-consuming process that seems to be much more case-based than an absolute theory capable of applying in all circumstances. The same approach was followed by the *Satamedia* case, where the judgments declare: 'In order to strike a balance between two different fundamental rights, the protection of the right to privacy requires that the limitations of Directive 95/46/EC in regard to data protection must apply where it is strictly necessary.[28]
3. The objective of the Regulation targets the main concern that matters to the legislator, which is prioritizing free movement of data over data protection (Art. 1 para. 3).[29]

1.2. Defensible argument.

Considering all factors above, the admissibility of e-evidence data in court is completely an alien subject to GDPR. Although the issue directly influences trial procedure, judgments' impartiality, and eventually the probable undermining of the right to a fair trial, the GDPR provides no guidance. Be that as it may, even though the admissibility test has been left blank in the EU legal framework, national courts in abiding by their domestic legal system, take charge of deciding whether the evidence should be suppressed in cases of illegal processes or not. Therefore, where a public body or law enforcement legally gathers sensitive data that is evidence of an imminent threat to public interest or security, there would be no perplexity since a clear-cut rule of law governs the matter. Conversely, a vexing dilemma emerges in a case where such evidence was obtained illegally and both parties are before a national court, struggling to overcome each other by bolstering their own baskets of evidence. In the scenario mentioned, the judge should first decide the validity

[27] Falling into semantic traps where the speaker mentions half-information (half-truth) and leaves the conclusion open to audiences has always been typical among people. Over time, this experience led to the coining of a pertinent proverb: '*qui tacet consentire videtur ubi loqui debuit ac potuit*,' which translates to 'He who is silent in a situation where he ought to have spoken and was able to, is taken to agree.' In parallel with this common understanding among people, different legal systems started to normalize legal conditions of silence and half-truths. Nowadays, almost all legal systems have codified the rule and encapsulated it in various sub-principles, such as misrepresentation and fraud. There are cases where silence might be a ground for recognizing implied consent; for instance, see *B.Shanmugam v. Thulasirama Reddy* S.A.No.495 (Madras 2011) (silence of counsel before the court), *Nottingham Patent Brick & Tile Co v Butler* [1886] 16 QBD 778 (CA) (half-truth may amount to misrepresentation).

[28] Judgment of 16 December 2008, *Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 56

[29] This reading from the third paragraph might be challenged in various ways due to its flexible tone. Nonetheless, it is noteworthy to mention that the free flow of data holds significant importance for GDPR as it has been allocated in the first article. On the other hand, the silence of the provision about balancing fundamental rights must not be overlooked.

and authenticity of the data and then examine the substantive issues of the case. The way in which a judge evaluates the admissibility of e-evidence has a direct influence on the EU's fundamental right to a fair trial. We suggest that this gray zone should not be solved by referring to GDPR, which does not deal with balancing fundamental rights. Up to now, it is perceivable that harmonizing right to data protection and the right to a fair trial must not be interpreted according to the provisions of the GDPR. However, in the next part, a reliable standard for courts and legal practitioners will be provided in order to resolve the quarrel.

2. Precedents of the ECtHR.

While EU legislation tends not to oversee the e-evidence admissibility issue, the current stance of the ECtHR (hereinafter, the court) system reveals a much more practical approach. However, the admissibility of a claim in the Court is completely different from admissibility of an evidence. The criteria for the latter has been enshrined in Article 35 ECHR.

The Court in order to assess the impact of procedural failings has established a test known of 'overall fairness'.[30] According to this test, the court must consider ten factors in order to determine the admissibility of evidence. The ten-factor test is designed to ensure that obtaining and presenting evidence at trial and procedural actions of domestic law enforcements do not jeopardize the accused's fundamental rights, notably the right to a fair trial (Art. 6 ECHR). The factors introduced by the court are as follows:

1. 'The court determines whether the applicant holds a type of physical or mental vulnerability;
2. The legal framework applied in pre-trial stage and the admissibility of evidence gathered at trial. In addition, the court should consider the chance of applying the exclusionary rule to inadmissible evidence, although it is unlikely that the whole proceeding will be considered unfair;
3. The opportunity to challenge the authenticity of the evidence and oppose its use;
4. Whether the evidence is reliable (quality of evidence), and the circumstances in which the evidence was obtained may raise doubt on its reliability, the court should also consider the nature and degree of any compulsion.
5. If the evidence was gathered unlawfully, the court should take into account the nature of the unlawfulness process and, where it violates other Convention Articles, also the nature of the violation.
6. In case where evidence is in the form of statement, the nature of the statement and whether it was immediately retracted or modified;
7. Evaluating the probative weight of the evidence, whether it forms an integral or significant part of probative evidence, and the strength of the other evidence in the case;

[30] *Beuze v. Belgium* [GC], 09 november 2018, no. 71409/10, § 150, ECHR 2018

8. Whether the evaluation of guilt was conducted by professional judges, lay jurors or lay magistrates. Also, any given direction or guidance made by them;
9. The existence of public interest and its weight in the prosecution and punishment of some specific offenses in issue;
10. Relevant procedural measurements given to domestic law or it's practice.'

The Court, however, has no tendency to evaluate validity of each piece of evidence. This is not the court's task.[31] In fact, the court practices its judicial capacity after the exhaustion of 'all domestic remedies'.[32] Nevertheless, the aforementioned test even though attempts to provide an overall fairness test, lacks in linking the domain of Article 6 (ECHR) [33] to Article 8 (ECHR) [34]. Nevertheless, up to now, the court's judicial records show a less supportive approach in order to establish a nexus between the two said rights. Most judges have so far overlooked the junction either by interpreting Art. 6 and 8 independently and ignoring the existence of any correlation between the two or by noting that the Convention does not address the admissibility issue of evidence due to its domestic essence.[35] On the contrary, the court in some specific areas has shown an extremely different perspective on protecting fair trial procedures. This often happens when the factual matrixes of a case hint at a breach of a law that could directly hamper the fairness of a trial. For instance, regarding the lawyer-client relationship (concerns about times of visit, access limitations, and the safety concerns of video conferences), [36] the court has intertwined the confidentiality of lawyer-client communications with the right to fair trial. In addition, while it is hard to discover the exact scope of Art. 6 due to its abstract wording, judges have tended to include various cases within the domain of a fair trial. Besides, the abstract wording of Art. 6 of the Convention did not hinder the court from further recognizing other look-alike scenarios in which fairness could be endangered. In doing so, the court has also successfully linked questioning the accused, confession, the right to remain silent, [37] inciting

[31] See *Vučković and Others v. Serbia*, 25 March 2014, no. 17153/11, § 69-77, ECHR 2014
[32] See Articles 13 and 35 (1) of the ECHR
[33] Related to 'right to a fair trial '
[34] Related to 'right to respect for private and family life'
[35] See the decision in *Bykov v. Russia* [GC], 10 March 2009, no. 4378/02, § 88, ECHR 2009 (the admissibility of evidence primarily falls within the national law regulations); *Khan v. the United Kingdom,* 12 May 2000, no 35394/97, § 34, ECHR 2000; *Schenk v. Switzerland*, 12 July 1988, no 10862/84, § 45, ECHR 1988; and *Moreira Ferreira v. Portugal* [GC], 11 July 2017, no. 19867/12, § 83, ECHR 2017-II.
[36] *Gorbunov and Gorbachev v. Russia*, 1 June 2016, nos. 43183/06 and 27412/07, § 37, ECHR 2016 (Lack of sufficient time for lawyer-client communications); *Salduz v. Turkey* [GC], 27 November 2008, no 36391/02, § 54, ECHR 2008 (Restriction on early access to lawyer); *Sakhnovskiy v. Russia* [GC], 2 November 2010, no. 21272/03, §§ 101,102, ECHR 2010 (limited time for lawyer to study the client's case file). *Öcalan v. Turkey* [GC], 12 May 2005, no. 46221/99, §§ 133, 135, ECHR 2005 (client's inability to consult a lawyer out of the hearing of a third party); *Rybacki v. Poland*, 13 April 2009, no. 52479/99, § 61, ECHR 2009 (safe and unhindered contacts of lawyers with their clients); *Moroz v. Ukraine*, 18 September 2017, no. 5187/07, § 68, ECHR 2017 (denial of private conversation between lawyer and client).
[37] *John Murray v. the United Kingdom* [GC], 8 February 1996, no. 18731/91, § 45, ECHR 1996; *Bykov v. Russia* [GC], no 4378/02, § 92, ECHR 2009.

suspects to commit crimes by entrapment,[38] and degrading treatments such as torture [39] (subject to Art. 3 of the Convention).[40]

In summary, it could be perceived from the above judgments that if a breach of legal duty is capable of significantly affecting the trial procedure, it is highly likely to establish a connection between the notions of Articles 6 and 8. Nonetheless, if the breach relates to privacy rights and not those mentioned earlier, the court tends not to overshadow the priority of delivering justice by excluding evidence obtained unlawfully. [41] It is remarkable to address here that many cases of the court merely deal with the tenor of the Art. 35 (1) ECHR. The procedural orders of the court necessitate a complaint to be meticulously cautious in bringing up his claim. If by any means, one of the admissibility requirements ignored, the court release itself from further examination of case and instantly makes its' mind to dismiss the case.[42]

---

[38] *Khudobin v. Russia*, 21 January 2007, no. 59696/00, § 128, ECHR 2006.

[39] *Jalloh v. Germany* [GC], 11 July 2006, no 54810/00, § 99, 105, ECHR 2006. The most relevant and unmentioned element in Article 6 ECHR, which is directly laid down in Article 14(3)(g) of the International Covenant on Civil and Political Rights, is the 'right against self-incrimination.' However, this is a 'generally recognized international standard,' and it might be the reason for the certainty of the court's rulings concerning discriminating treatments. See T Thienel, 'The Admissibility of Evidence Obtained by Torture under International Law' (2006) 17 EJIL, 349, 356.

[40] For a more elaborated list of case laws, see Council of Europe, Guide on Article 6 of the European Convention on Human Rights, updated on 31 August 2020, pp. 41, 44-47, 92-93, available at <https://www.echr.coe.int/documents/d/echr/guide_art_6_criminal_eng > accessed 09 February 2024.

[41] This approach echoes the old edict of '*Fīat iūstitia ruat cælum*' which suggests that justice must be done regardless of any consequences it may have. The famous axiom '*Justice must not only be done, but must also be seen to be done*' laid down by Lord G. Hewart also reflects the high public demand for delivering justice. For more useful explanations on the literature and relevant topics to the dictum, see A R Oakes and H Davies, 'Justice Must Be Seen to be Done: A Contextual Reappraisal' (2016) 37 ADLR 461. The applicable sphere of the dictum, moreover, has already been highlighted by Art. 6 of the ECHR; see Justice Committee of the House of Commons, *Public opinion and understanding of sentencing: Government and Sentencing Council responses to the Committee's Tenth Report of Session 2022–23*, (2024-01, HC 442) 2.

[42] For instance, see *Schenk v. Switzerland*, 12 July 1988, no. 10862/84, § 47, ECHR 1988. In a recent case, one of the main justifications of the judgement was that defendant had not used the opportunity to challenge the authenticity of incriminating evidence. in a case where the applicant, who was an employee (a medical representative) of the defendant (a pharmaceutical company), filed a complaint with the National Data Protection Commission (CNPD) in regard to breach of private data committed by the company through the installation of GPS in employees' vehicles. Subsequently, the CNPD did not affirm any privacy infringement. The applicant then challenged the decision, but the CNPD reaffirmed the previous resolution. In 2014, the company dismissed the applicant due to the outcome of a disciplinary proceeding based on the accusation that the applicant had manipulated the installed GPS to reduce the traveled distance and therefore evade the company's travel limitations. Consequent to the justification made by the first instant court and the Court of Appeal for his dismissal, he eventually, in 2016, lodged a complaint before the ECtHR, where four judges unanimously held that the signed agreement between the company and the applicant, by its wording clearly grants the company the right to monitor the travelled distance of the employees by installing GPS. Despite this, the Court stated that all the obtained geolocation data are not valid since some of those data consist of monitoring the applicant's professional activities. The Court, nevertheless, to evaluate whether there was an infringement or not, somehow absolved its duty by indicating that the applicant had enough opportunity to avert his dismissal by challenging the domestic court's decision. Following this vindication, the Court concluded that the use of GPS in the case did not undermine the principle of fair trial under Art. 6(1) of the ECHR. See paragraphs 4-26, 132, 142 and 145 of the case. The court, however, did not exclude the evidence gathered by GPS. See *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 13 December 2022, no. 26968/16-2022, ECHR 2022. Furthermore, the judgment in *Uzun v. Germany* also considers whether geolocation data gathered during governments' surveillance measurements were valid. The court stated that, in accordance with the case law of the court, Article 8(2) of the Convention, notably the phrase 'the law' therein, should be interpreted in the sense that the measurements must have some basis in domestic law. See *Uzun v. Germany*, 2 December 2020, no. 35623/05, § 60, ECHR 2010.

[42] Beuze v. Belgium (n. 27) 150 (C).

Regardless of the articulated situations where the court has a clear standpoint, [43] the delimitation of the applicable scope of fair trial and illegitimate evidence gathering has yet to be explored.

2.1. Discourse about the role of e-evidence.

Back to e-evidence, the literature of the Court is even more blurry than expected. However, among the sparse literature available, there are some unproductive discussions that do not contribute to mapping out boundaries for the present debate. Nevertheless, the reluctance of the court in broaching a general test is noticeable in concurring opinion of Judge Cabral Baretto in case of Bykov v. Russia[44] where he states:

'I find it regrettable that the Grand Chamber missed the chance to elucidate once and for all an issue which has made the Court for a long time to challenge: whether the use of evidence obtained in breach of Article 8 of the Convention and used in criminal proceedings undermines the fairness of a trial as assured by Article 6'.[45]

Bykov v. Russia deals with covert operation of Federal Security Service of the Russian Federation (FSB) to obtain evidence that proves Bykov intended to murder 'S.'. In this case police instructs a third person (V.) to carry on hidden radio-transmitting device join the applicant in a guest-house where he was residing. After all, V. opened assassination discussion with the applicant, and pretended he himself conducted the crime. To persuade the applicant, V. showed him some evidence such as a watch belonging to S. Ending their chat, V. received a reward in cash as previously suggested by the applicant. In recourse of the applicant to the Court after passing over national procedural, the court recognized that conducting covert listening constitutes a breach under Article 8 of the Convention.[46] Nevertheless, this does not render the obtained evidence illegal in case to meet the requirements of Article 6 (1). Finally, the court in respect of non-pecuniary damages awards the applicant 1000 Euros (which was 118,089.25 lower than his request)[47]. Moreover, the court also found a breach of Article 5 (3) Convention due to excessively long pre-trial detention (20 months and 15 days).[48] Very alluring point of the judgment is where the court emphasizes on the up-hand position of Article 8 Convention in interpreting national laws.[49] The Court stated:

---

[43] See notes 33-37.
[44] *Bykov v. Russia* [GC], 10 March 2009, no. 4378/02, ECHR 2009.
[45] Ibid Concurring Opinion of Judge Cabral Baretto. Also see Concurring Opinion of Judge Kovler in the same case.
[46] Ibid, *Bykov v. Russia* (n 41) § 91
[47] Applicant claimed 4,059,061.80 Russian Roubles (119,089.25 euros) for both pecuniary and non-pecuniary damages. See Ibid, *Bykov v. Russia* (n 41) § 108
[48] Ibid, *Bykov v. Russia* (n 41) §67.
[49] Russian Government tried to legalize the covert surveillance by a literalism approach towards Article 8 of Operational-Search Activities Act of 12 August 1995(national legislation). The Article provides: 'Operational-search activities involving interference with the constitutional right to privacy of postal, telegraphic and other communications transmitted by means of wire or mail services, or with the privacy of the home'. Defendant, however argued that the means of their operation (radio-transmission) was neither wire or mail, therefore the action was legitimate, and even if it is covered by the said Act the 'gust-house' is not considered 'the home' in the article. On the contrary, the court observed the action contrary to law and

'The phrase 'in accordance with the law' must be interpreted with respect to the quality of law in associate with the compatibility to the rule of law. In addition, national law should clearly provide adequate indication for individuals the circumstances in which public agents might be entitled to take covert measures'.[50]

Alongside all the mentioned facts and two breaches of the Convention, the Court appraises the fairness of trial by highlighting following factors and finds no violation of Article 6(1) of the Convention:

'1) The applicant was free to receive V. 2) Not only he was free not talking to V. but also he himself was willing to do so because of his personal interest, 3) The Domestic court did not merely examine the transcript of the record, instead they have considered the expert view in order to assess the applicant's relationship with V. and the method in which he involved in the conversation.'[51]

Astonishingly, while the facts of the case clearly orient readers to 'third-party consent search' doctrine, the judgments avoid any illustrative examination in this regard. Whether, V. had a shared privacy in respect to his conversation with S. or the carried out action on behalf of the government would be flagged as illegal entrapment remained silent. [52]

2.2. What has been done so far?

To our knowledge, the issue has not yet been explored by ECtHR, and there is no benchmark guideline for the issue at hand. As mentioned earlier, the ECtHR still suffers from a lack of relevant cases, and no judicial opportunity has yet come to seize the matter, considering the issue in ample detail. Some legal systems, such as many states in the USA, have a solid background in judicial adjudications concerning violations of the 4th Amendment (unreasonable search and seizure).[53] Some countries have also granted wide discretion to courts in order to suppress illegally obtained evidence.[54] Nonetheless, the ECtHR tends to confine its authority to interfere in domestic procedures and does not overwhelm national prosecutory investigations owing to ill-privacy

found no sense in assessing further condition (values of democratic society) set out by Art. 8(2) Convention. See, Ibid, *Bykov v. Russia* (n 41) § 61-83.

[50] Ibid, (n 41) §§ 76 and 78.

[51] Ibid, (n 41) §§102 and 103.

[52] However, the issue of entrapment was addressed by Partly Dissenting Opinion of Judge Costa, Judge Spielmann joined by Judges Rozakis, Tulkens, Casadevall and Mijović.

[53] For instance, to see cases related to outside-warrant measurements: *United States v. Abbell* 963 F. Supp. 1178 (S.D. Fla. 1997); *United States v. Upham* 168 F.3d 532 (1st Cir. 1999) para536; *United States v. Carey* 172 F.3d 1268 (10th Cir. 1999); *United States v. Walser* 275 F.3d 981, 987 (10th Cir. 2001). Seemingly, there is a rapid growth in cases related to Amendment 4; to see the list of recent cases, turn to: R J. Hedges (Editor), 'Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials' (2022), <https://www.mass.gov/doc/electronic-evidence-in-criminal-investigations-and-actions-april-2022/download> accessed on 19 May 2024.

[54] Article 78(1) of the Police and Criminal Evidence Act 1984 grants courts the power to suppress any evidence if their entrance into the case would have such an adverse effect on the fairness of trial. For instance, in a case where a 19-year-old girl was accused of manslaughter, the appeal court quashed all the confessions of the accused. The court, however, justified this decision based on the granted discretion of Article 78 and due to the fact that the accused had been refused access to her lawyer in her first investigatory interview. Therefore, in the court's view, the lack of this right in her first interrogation had affected all subsequent decisions and confessions. See, R v McGovern 92 Cr. App. R 228 (App1991).

safeguards or infringements. It seems the Court cannot designate the tight relationship between Articles 6 and 8.

2.3. Defensible argument.

As seen in *Beuze v. Belgium* [55], the judgment laid down a non-exhaustive list comprising ten factors. However, the offered suggestion has three drawbacks, which hinder its effectiveness and future applicability. First and foremost, the provided guideline is not palpably measurable by the Court. The fifth assessment requires the Court to weigh the unlawfulness of the evidence-gathering processes and any violation of the Convention's provisions. However, how future judgments could evaluate the nature and weight of unlawful actions or the strength of some human rights over others is not clear. Secondly, the seventh factor of the test does not clarify whether the Court should suppress those illegally obtained evidence that forms the significant probative part of proofs or should allow them. Each will result in different outcomes; supposedly, if the only evidence of the claimant's conviction is found illegitimate during the Court's assessment, allowance and suppression represent dissimilar viewpoints upon fairness of a trial. If the sole evidence is the product of illegal government surveillance, suppression could in some scenarios undermine the public interest [56] and no reasonable person would likely agree on this hypothetical equilibrium wherein a society is endangered by a potent risk, but the Court rejects delivering justice because of a trivial outside-warrant action by a police officer. Not to mention that it is quite imaginable that the infringement of privacy might not be at all a matter of interest for the accused, but he wills to use his right in order to try his chance and dismiss the case. However, if there are several evidences in a case and the first piece of evidence was afforded in an illegitimate way, the second piece (correlated or irrelevant to the subject of the first) must be suppressed in order to protect the fundamental rights of the accused (in case there is no opposing interest from the public community). Moreover, the Court should distinguish between the two following orders in gathering supportive evidence: first, if legitimate-looking evidence stems from an illegitimate measurement or evidence which was itself a product of illegal action, all further evidence (no matter whether correlated to the first or not) must be disregarded by applying the exclusionary rule.

[55] See, *Beuze v. Belgium* (n 27) §150 (C).
[56] See Article 1 of the Convention. The weakness of the seventh factor relies on common understanding since people completely overlook the quantity of evidence where there is an immense threat to public interest, for example, in cases of severe crimes.

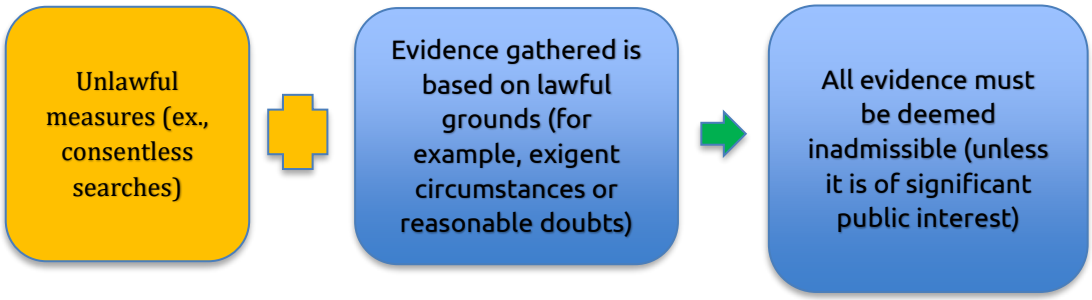


Figure A

For instance, a police officer, based on a consent provided by a premise owner, starts searching the consented areas; however, the officer goes further and searches other areas as well (such as the owner's laptop) and finally discovers digital evidence of a crime (related or irrelevant to the reason for the search). Since there was no consent to allow officers to search the landlord's laptop, the obtained evidence should be suppressed.[57] Even if the second evidence appears legitimate at first glance, the circumstances that gave rise to obtaining further evidence were due to the conduct of an unlawful measure. (see, Figure-A) on the other hand, if the chain of evidence started with legitimate discovery, and ended in illegitimate findings, the latter would not invalidate the earliest findings. (See, Figure B).[58]

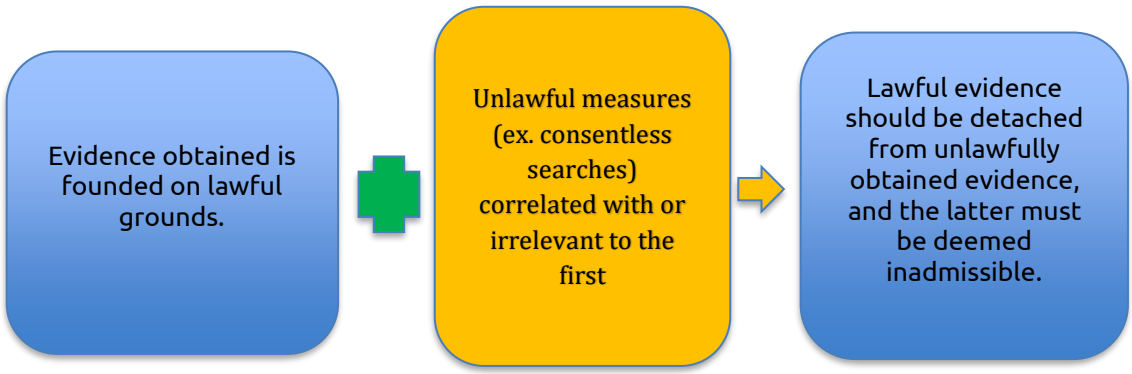


Figure B

[57] This example is inspired by a real case where a dweller of a premise (Turner) consented to two detectives searching his premise. The consent given was to help detectives find the person who assaulted Turner's neighbor (Mrs. Thomas). Nevertheless, Mr. Turner was not a suspect, but since his home was located next to Mrs. Thomas's, the detectives were concerned about the possibility that the intruder might have fled into Turner's apartments. In the middle of the investigation, while Turner was talking to one of the detectives downstairs, another detector started checking Turner's laptop and discovered many pieces of data related to child pornography. The court, however, called all evidences invalid based on the Fourth Amendment, and justified the ruling by remarking that Turner did not consent to the computer search and neither had the opportunity to object to the search. *United States V. Turner* 169 F. 3D 84, United States Court of Appeal, (1 Cir, 1999) para 87-89. Also see *United States v. Carey* 172 F.3d 1268 (10th Cir. 1999) para 1270-1272 wherein a detective had been appointed for drug investigation and tasked with discovering any related evidence of drug transactions through searching JPG files on the defendant's computer. However, he did not find any pertinent evidence; rather, he found 244 JPG files containing child pornography.

[58] This scenario is similar to a situation where an investigator has already found some legal evidence but further expands his search domain and extends the sphere of the warrant. For instance, if in the said scenario, the detective could have found some drug evidence and afterwards expanded his action regardless of the specifications of the warrant, this could be an example of when illegitimate actions follow legitimate ones.

Therefore, the proposed guideline in *Beuze v. Belgium* should be revised as follows in modification of the 7th test:

'7-The court must evaluate the probative weight of the evidence by determining whether the suppression of evidence would challenge the interests of society. However, if any afforded lawful evidence supports the illegal evidence, the court must orderly assess the correlation between them. If lawfully obtained evidence is the result of illegal evidence (or measurement), in case there is no significant interest of the public, the court should reject all evidence'.

Conclusion.

The perplexities in admissibility issues are often associated with the wide power of national jurisdictions in interpreting relevant legal provisions, which enhances the complexity of the riddle. In interpreting the GDPR or derived national standards, courts should consider that the said regulation does not develop any balance between inconsistent fundamental rights. Not to mention that striking a balance that links two or more fundamental rights is a backbreaking task to be carried out and often deemed to fail due to the lack of suitable gratification from legal practitioners and societies. This paper suggested that the ten-factor test addressed in the judgment of Beuze v. Belgium (2018) could serve as a yardstick for further national judgments as well as ECtHR future procedures. In the absence of any national law establishing a balance between the right to a fair trial and the right to protection of personal data (or the right to privacy as followed by the ECHR), member states of the European Union shall adhere to the aforementioned guideline of the Court. As a result of this adherence, not only an internal EU-level harmonization will be reached, but members will also, in the meantime, protect EU fundamental rights and comply with the spirit of the union's legislation, namely those enshrined in the Charter and other EU law principles. However, the paper further criticized some factors of the provided test, which it realized may expose a manifest injustice to the parties to a dispute. Finally, the paper modified the test in the judgment's seventh factor, as follows:

'The court must evaluate the probative weight of the evidence by determining whether the suppression of evidence would challenge the interests of society. However, if any afforded lawful evidence supports the illegal evidence, the court must orderly assess the correlation between them. If lawfully obtained evidence is the result of illegal evidence (or measurement), in case there is no significant interest of the public, the court should reject all evidence'.

Drev M, Stanimirović D, Delak B, 'Meta-analysis of privacy legal framework: revising the various approaches for balancing privacy risks and usability of healthcare information systems' (2024) 2 EJPLT, 221 – 232.
DOI: https://doi.org/10.57230/EJPLT242MDDSBD

EJPLT
ISSN 2704-8012



Meta-analysis of privacy legal framework: revising the various approaches for balancing privacy risks and usability of healthcare information systems

Meta-analisi del quadro normativo sulla privacy: *revisione dei differenti approcci per bilanciare i rischi per la privacy e l'usabilità dei sistemi informativi sanitari*

MATJAŽ DREV
Information security consultant, Ph.D., Center for Healthcare Informatics, National Institute of Public Health

DALIBOR STANIMIROVIĆ
Associate Professor, Ph.D., Faculty of Public Administration University of Ljubljana

BOŠTJAN DELAK
Assistant Professor, Ph.D., Faculty of information studies in Novo Mesto

Abstract

The integration of information and communication technologies with advanced machine learning, or artificial intelligence, brings both benefits and risks. These risks are particularly relevant in the context of personal data protection in healthcare, where non-compliance with legal requirements can lead to severe consequences for patients and substantial fines for healthcare institutions. A proactive approach to managing these risks involves the use of privacy by design frameworks and conceptual tools. This paper presents an overview of key privacy framework, highlighting their potential to deepen theoretical understanding and support the development of conceptual models that may enhance data protection in healthcare. Using qualitative and comparative research focused on content analysis, this study examines the role of these frameworks in embedding privacy principles within organizations. While primarily theoretical, the findings provide deeper insights into the principles underlying information privacy and lay a foundation for practical applications, such as testing frameworks through case studies to improve privacy compliance.

© The author(s) 2024, 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'integrazione delle tecnologie dell'informazione e della comunicazione con l'apprendimento automatico avanzato, o intelligenza artificiale, comporta vantaggi ma anche rischi. Tali rischi sono particolarmente rilevanti nel contesto della protezione dei dati personali in ambito sanitario, dove la mancata conformità ai requisiti normativi può portare a gravi conseguenze per i pazienti e a sanzioni elevate per le istituzioni sanitarie. Un approccio proattivo alla gestione di questi rischi prevede l'utilizzo di quadro normativo e strumenti concettuali di privacy by design. *Questo articolo presenta una panoramica del quadro normativo di riferimento per la* privacy, *evidenziando il suo potenziale per approfondire la comprensione teorica e sostiene lo sviluppo di modelli concettuali che possano migliorare la protezione dei dati in ambito sanitario. Utilizzando una ricerca qualitativa e comparativa incentrata sull'analisi dei contenuti, questo studio esamina il ruolo del* privacy framework *nel radicare i principi della* privacy *all'interno delle organizzazioni. Pur essendo principalmente teorici, i risultati forniscono approfondimenti sui principi alla base della* privacy *delle informazioni e gettano le basi per applicazioni pratiche, come la sperimentazione dei* framework, *attraverso casi di studio per migliorare la conformità alla* privacy.

Keywords: personal data; data protection; privacy by design; privacy frameworks; meta-analysis; healthcare information systems

Summary: 1. Introduction. – 2. Methods. – 2.1. Literature review. – 2.2. Comparing frameworks. – 2.3. Building a model. – 3. Results. – 4. Discussion. – 5. Conclusions.

1. Introduction

In contemporary society, increasing emphasis is placed on personal data protection.[1] This importance is an expression of respect for individual privacy and also a way to ensure compliance with legal requirements. Such compliance became particularly important in the European Union (EU) after the introduction of the General Data Protection Regulation (GDPR).[2] The USA has proposed American Data Privacy and Protection Act (ADPPA) which is still in legislative phase [3] ;however, an increasing number of states, for example, California, Virginia, Colorado, Connecticut, and Utah [4] have adopted information privacy laws.

One particular feature of GDPR is promoting the concept of privacy by design, which originates from Ann Cavoukian's influential essay.[5] The basic idea is to use different principles to shape the development and use of Information

[1] B Custers, G Malgieri, 'Priceless Data: Why the EU Fundamental Right to Data Protection is at Odds with Trade in Personal Data' (2022) 45 Comput Law Secur Rev 83.
[2] J Ruohonen, K Hjerppe, 'The GDPR Enforcement Fines at Glance' (2022) 106 Inf Syst 76.
[3] A Quay, 'Desperation for Legislation: The Need for the American Data Privacy and Protection Act' (2024) 41(4) Wis. Int'l L. J. 707.
[4] F Bellamy, 'U.S. Data Privacy Laws to Enter New Era in 2023' (2023) <https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/> accessed 16 May 2024.
[5] A Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (2009) https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 1 March 2024.

Communication Technology (ICT) in a way that interferes as little as possible with the privacy of individuals. However, Gurses, Troncoso, and Diaz[6] pointed out that the principles of privacy by design set by Cavoukian are vaguely defined and therefore unsuitable for use in developing frameworks and conceptual tools.

During our attempt to develop a conceptual model of privacy by design, which would be concise enough to use in case studies, we had to explore other approaches on how to implement privacy principles into the design and use of ICT. Through research, we found that substantial work has already been done. Recent developments worldwide in the misuse of personal data and unauthorized intrusions into information systems have heightened global awareness and intensified the debate around data protection.[7] These incidents underscore the critical importance of understanding and embedding privacy principles at every stage of information system development. As a result, data privacy is increasingly viewed as a foundational component rather than an afterthought, prompting organizations and policymakers alike to prioritize the integration of robust security protocols and privacy frameworks.[8] This shift encourages the adoption of privacy by design approaches and drives the development of frameworks that help ensure personal data is safeguarded against emerging threats and unauthorized access. It also became clear that efforts to develop privacy by design continue at an accelerated pace.[9,10]

Based on a meta-analysis of different approaches, we determined the building blocks for a conceptual model and successfully tested it on several case studies within the healthcare sector. Results were encouraging and were published in two articles.[11,12] However, this paper will not go into detail on how we developed the conceptual model but is rather a summary of extensive meta-analyses of different privacy frameworks that already exist. These frameworks provide a solid foundation for further developing the idea of privacy by design and conceptual tools that can put this idea into practice.

The paper is organized as follows. In the next section, we shortly review the literature and compare the frameworks with model presentation. Section three present the results, followed by discussion and concluding remarks.

---

[6] S Gürses, C Troncoso, C Diaz, 'Engineering Privacy by Design' (2011) <https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf> accessed 24 July 2024.

[7] JM Kizza, 'System Intrusion Detection and Prevention' in *Guide to Computer Network Security*, Texts in Computer Science (Springer, Cham, 2024).

[8] LL Dhirani and others, 'Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review' (2023) 23(3) Sensors, 1151.

[9] C Kurtz, M Semmann, T Böhmann, 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors' (AMCIS 2018 Proceedings, New Orleans, Louisiana, 2018).

[10] FH Semantha and others, 'A Systematic Literature Review on Privacy by Design in the Healthcare Sector' (2020) 9 Electronics 452.

[11] M Drev, B Delak, 'Conceptual Model of Privacy by Design' (2021) 62(5) J Comput Inf Syst 888.

[12] M Drev, D Stanimirović, B Delak, 'Implementation of Privacy by Design Model to an eHealth Information System' (2022) 10(1) Online J Appl Knowl Manag 77.

2. Methods.

2.1 Literature review.

Though the original concept of privacy by design is attributed to Ann Cavoukian`s essay "Privacy by Design: The 7 Foundational Principles",[13] which was published in the 1990s, the basic idea of implementing privacy concerns into existing and new ICT is even older. In the 1980s, authors such as Denning[14] and Chaum [15] wrote about concerns regarding the erosion of information privacy and ways to protect it through specific design of ICT. This approach later evolved into a privacy framework called "privacy enhancing technologies" (PETs).[16] Extensive meta-analyses of research work on privacy by design were made by Kurtz et al.[17] and Semantha et al.[18] In both studies authors examined how often the phrase "privacy by design" appeared in the titles, abstracts, or keywords of scientific articles. They reviewed the following databases: ACM Digital Library, AISeL, EBSCO Business Source Complete, EBSCO EconLit, IEEEXplore, ProQuest, CDU library, and ScienceDirect.

During the last two decades, different attempts were made to either build on the original idea of privacy by design or develop new approaches. Authors such as Spiekermann and Cranor,[19] Gurses et al.,[20] Hoepman,[21] Colesky et al.[22] and Nguyen & Tran,[23] focused on procedural aspects of information privacy protection. This was similar to the concept of "Privacy Impact Assessment" (PIA) which emphasized a project-based and systematic approach to the protection of personal data. PIA was mainly developed by Bennet,[24] Clarke,[25] Cavoukian[26] and De Hart and Papakonstantinou.[27] It also became part of the

[13] A Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (n 4).
[14] DE Denning, *Cryptography and Data Security* (Addison-Wesley Publishing Company, Boston, USA, 1982).
[15] D Chaum, 'Security without Identification Card Computers to Make Big Brother Obsolete' (1985) 28 Commun ACM 1030.
[16] GM Garrido and others, 'Revealing the Landscape of Privacy-Enhancing Technologies in the Context of Data Markets for the IoT: A Systematic Literature Review' (2022) 207 J Netw Comput Appl, 103465.
[17] C Kurtz, M Semmann, T Böhmann, 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors' (n 7).
[18] FH Semantha and others, 'A Systematic Literature Review on Privacy by Design in the Healthcare Sector' (n 9).
[19] S Spiekermann, LF Cranor, 'Engineering Privacy' (2009) 35 IEEE Trans Softw Eng 67.
[20] S Gürses, C Troncoso, C Diaz, 'Engineering Privacy by Design' (n 5).
[21] JH Hoepman, 'Privacy Design Strategies' (2014) IFIP International Information Security Conference 446.
[22] M Colesky, JH Hoepman, C Hillen, 'A Critical Analysis of Privacy Design Strategies' (2016) Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops 33.
[23] MT Nguyen, MQ Tran, 'Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of Legal and Regulatory Frameworks Impacting Cybersecurity Practices' (2023) 6(5) Int J Intell Autom Comput 87.
[24] C Bennett, *The Privacy Impact Assessment Handbook* (2007) https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/09/PIAhandbookV2.pdf accessed 2 February 2024.
[25] R Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Comput Law Secur Rev 123.
[26] A Cavoukian, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers* (2011) <http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf> accessed 27 January 2024.
[27] P De Hert, V Papakonstantinou, '*Transparency in the European Data Protection Regulation: Implications for Privacy Impact Assessments'* (2016).

GDRP, albeit under the abbreviation Data Protection Impact Assessment (DPIA).[28]

With the rapid advancement of ICT, the increasing interconnectedness of information systems, and the rising need to address and prevent security risks, several alternative approaches have been explored. Hoepman[29] emphasized the importance of privacy protection strategies, distinguishing between data-oriented and process-oriented strategies. Foukia et al.[30] developed the privacy protection framework PISCES, Jensen et al.[31] developed STRAP, Kalloniatis et al.[32] developed PRIS, and Piras, L. et al.[33] developed DEFeND Architecture. The Federal Trade Commission developed Fair Information Practice Principles (FIPP) which are similar to GDPR's basic principles. The European Commission formed a consortium of 11 research institutions and started project PRIPARE. Within the project, review of existing privacy methods was done, and the result was the publication of the guidelines "PRIPARE Handbook - Privacy and Security by Design Methodology" which included practical instructions for ICT developers.[34]

Important contributions were made by the International Standard Organization (ISO) with the development of standards such as ISO/IEC 27701:2019 which translates GDPR provisions into a precise control list and ISO/IEC 29100:2011, which provides guidelines on how to implement PIA into data processing operations. In this context, standard ISO/IEC 27001:2022 should also be mentioned, as it provides a comprehensive information security control list. In the context of guidelines, in 2020 National Institute of Standards and Technology (NIST) issued "The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management".[35]

2.2 Comparing frameworks.

Through the meta-analysis of contributions made by previously listed authors, the main privacy by design frameworks were defined: GDPR, PET, PIA, FIPP, and Privacy Strategies. These frameworks were analyzed in more detail to compare their strengths and weaknesses (Table 1).

---

[28] G Georgiadis, G Poels, 'Towards a Privacy Impact Assessment Methodology to Support the Requirements of the General Data Protection Regulation in a Big Data Analytics Context: A Systematic Literature Review' (2022) 44 Comput Law Secur Rev 105640.

[29] JH Hoepman, 'Privacy Design Strategies' (n 20).

[30] N Foukia, D Billard, E Solana, 'PISCES: A Framework for Privacy by Design in IoT' in Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST) (2016, Auckland, New Zealand).

[31] C Jensen and others, 'STRAP: A Structured Analysis Framework for Privacy' https://www.academia.edu/62138420/Strap_A_structured_analysis_framework_for_privacy accessed 12 May 2024.

[32] C Kalloniatis, E Kavakli, S Gritzalis, 'Addressing Privacy Requirements in System Design: The PriS Method' (2008) 13 Requir Eng 241.

[33] L Piras and others, 'DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance' in Proceedings - 16th Trust, Privacy and Security in Digital Business International Conference 2019 (2019) 78.

[34] PRIPARE Project, *PRIPARE Handbook - Privacy and Security by Design Methodology* (2016) http://priparepreject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf accessed 7 May 2024.

[35] NIST, *The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (2020) https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf accessed 23 May 2024.

However, regarding the selection of frameworks, additional explanations should be added. The selection was to some extent guided by the requirements of the primary research project – the development of the privacy by design model. As this model was intended to be used by EU organizations for monitoring and improving compliance with European legal requirements, GDPR was chosen as a baseline. Although comparison of GDPR with other legal frameworks such as the ADPPA, California Consumer Privacy Act (CCPA), China's Personal Information Protection Law (PIPL)[36], Brazil's General Data Protection Law (LGPD), or Japan's Act on the Protection of Personal Information (APPI), would seem more appropriate and could offer new insights, comparative legal approach was not necessary for the primary purpose of developing the conceptual model. On the other hand, assessing if GDPR includes elements of other methodological approaches to privacy by design, was necessary.

Table 1: Comparison of privacy by design frameworks

	GDPR	PET	PIA	FIPP	Privacy Strategies
Characteristics	A binding legal document that organizations in the EU must comply with. It contains procedural and technical dimensions of personal data protection.	Recommendations for using IT in a way that ensures the least intrusion into privacy. Emphasis on anonymization, data obfuscation, and encryption techniques.	Recommendations for the design of personal data processing operations in such a way that the privacy of individuals is protected as comprehensively as possible. The focus is on procedural aspects of data protection. It includes the use of tools such as the decision tree and the data circle. It emphasizes the importance of risk analysis.	Recommendations that are followed primarily in the US, not in the EU. Very similar in content to GDPR, they mainly cover legal and to some extent organizational aspects, not much focus on security. Emphasis on the minimization of data processing, transparency, informing individuals, and protecting the right to choose.	Data oriented strategies are similar in content to the PET framework, which emphasizes detailed technical approaches to achieve anonymization, obfuscation, and encryption of data. Process oriented strategies, on the other hand, are similar to frameworks such as PIA and FIPP by emphasizing data control, the possibility of exercising data rights, and ensuring compliance.
Advantages	Applicable legal regulation. Violations are sanctioned by supervisory authorities. A comprehensive approach to the protection of personal data. Legal aspects of data protection are described in detail.	Strong focus on the technical aspect of data protection. A detailed description of IT methods for achieving data obfuscation.	Its recommendations are formally included in GDPR. A comprehensive, proactive, systematic, and transparent approach to the protection of personal data.	The framework is similar in content to GDPR, relatively comprehensive approach, an emphasis on legal and organizational dimensions of data protection. Focus is on the protection of the right individuals.	Data and process oriented strategies fully cover all aspects of personal data protection.
Weaknesses	The procedural aspects of data protection are not defined and described in detail. Security (technical) aspects of personal data protection are not defined and described in detail.	These are non-binding recommendations. The technical aspects of data protection are taken into account, but not much consideration is given to the legal and organizational dimensions.	There are no particular disadvantages, PIA as an approach is already included in the GDPR. The PIA itself is not binding, except in the segment covered by the GDPR.	This framework is general and less comprehensive than the GDPR, taking into account selected legal and organizational aspects, but not the technical aspects of personal data protection. FIPPs are less binding than GDPR, they apply mainly in the USA, not the EU.	These are partial and scattered approaches made by different authors, which are less coherent and condensed than, for example, the PIA framework. These approaches are not mandatory for organizations.

[36] PA Weber, N Zhang, H Wu, 'A comparative analysis of personal data protection regulations between the EU and China' (2020) 20 Electronic Commerce Research 565–587.

2.3 Building a model.

After reviewing and comparing the selected privacy frameworks, we had to choose one and use it for designing a conceptual model. As our effort was focused on providing tools for achieving compliance with GDPR requirements, that framework proved itself most suitable for our needs since the model was intended to be used primarily on EU organizations. Also, the approach that GDPR takes on data protection is relatively holistic[37], it takes into account both legal, organizational, and security aspects. Building upon the GDPR framework, it was necessary to determine individual building blocks that should make up the model. In this regard, a meta-analysis conducted by Huth and Matthes[38] proved most useful (Table 2). They reviewed research by Bellotti and Sellen,[39] Hong et al.,[40] Jensen et al.,[41] Kalloniatis et al.,[42] Spiekermann and Cranor,[43] Deng et al.,[44] Hoepman,[45] and Notario et al.[46] Their goal was to determine whether; by comparing different studies, it is possible to determine the general building blocks that define privacy by design.

Table 2: Presence of privacy by design elements in the contributions of selected authors.[47]

Analyzed paper / presence of privacy by design elements Legend: ● – element present ◐ – element partially present ○ – element not present	**Pseudonymity**	**Unlinkability**	**Access control authorization**	**Integrity**	**Confidentiality**	**Accessibility**	**Data minimization**	**Transparency of processing**	**Storage limitation**	**Purpose limitation**	**Accountability**	**Encryption**

[37] A Datoo, 'Data in the post-GDPR world' (2018) 9 Computer Fraud and Security 17–18.
[38] D Huth, F Matthes, 'Appropriate Technical and Organizational Measures: Identifying Privacy Engineering Approaches to Meet GDPR Requirements' (2019) AMCIS 2019 Proceedings 1790.
[39] V Bellotti, A Sellen, 'Design for Privacy in Ubiquitous Computing Environments' in Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW '93 (1993) 77 https://doi.org/10.1007/978-94-011-2094-4_6 accessed 2 May 2024.
[40] J Hong and others, 'Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems' (2004) Proceedings of the 2004 Conference on Designing Interactive Systems Processes, Practices, Methods, and Techniques - DIS '04 91 <https://doi.org/10.1145/1013115.1013129> accessed 11 January 2024.
[41] C Jensen and others, 'STRAP: A Structured Analysis Framework for Privacy' (n 30).
[42] C Kalloniatis, E Kavakli, S Gritzalis, 'Addressing Privacy Requirements in System Design: The PriS Method' (n 31).
[43] S Spiekermann, LF Cranor, 'Engineering Privacy' (n 18).
[44] M Deng and others, 'A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements' (2011) 16 Requir Eng 3.
[45] JH Hoepman, 'Privacy Design Strategies' (n 20).
[46] N Notario and others, 'PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology' in Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015 (2015) 151.
[47] D Huth, F Matthes, 'Appropriate Technical and Organizational Measures: Identifying Privacy Engineering Approaches to Meet GDPR Requirements' (n 35).

Bellotti and Sellen, 1993	○	○	○	○	○	○	○	●	○	●	●	○
Hong et al., 2004	●	○	●	○	●	○	○	●	●	●	○	○
Jensen et al., 2005	○	○	○	●	●	●	●	●	●	○	●	●
Kalloniatis et al., 2008	●	●	●	●	●	●	○	○	○	○	○	●
Spiekermann and Cranor, 2009	●	●	●	○	○	●	●	●	○	●	●	●
Deng et al., 2011	●	●	○	○	●	○	●	●	◐	◐	●	●
Hoepman, 2014	●	●	●	●	●	●	●	●	●	●	●	●
Notario et al., 2015	○	○	○	●	●	●	●	●	●	●	●	◐

The findings of a comparative analysis conducted by Huth and Matthes[48] suggest a certain universality of privacy by design elements, which is encouraging for any effort to create a model that is general enough to be used in a variety of personal data processing contexts and specific enough to be introduced into personal data processing operations within a reasonable time frame.

3. Results.

In our effort to design a conceptual model, we attempted to connect basic principles of privacy by design as set by Ann Cavoukian[49] with the GDPR privacy framework and the set of building blocks identified as common across different approaches by Huth and Matthes (Table 3).[50]

Table 3: Comparison of three approaches to understanding privacy by design.[51]

Basic principles (Ann Cavoukian, 2009)	GDPR framework	Comparative analysis (Huth and Matthes, 2019)
Proactivity	DPIA	/
Privacy as default	Basic principles of the GDPR (Article 5)	Transparency of processing, minimum scope of processing, limitation of data retention, limitation of the purpose of processing
Privacy built into the design of the solution	Default and built-in data protection (Article 25)	Pseudonymization, non-connectivity, minimum scope of processing, limitation of data retention, limitation of purpose of processing, liability
Full functionality	/	/
Data security throughout the entire processing cycle	Security of personal data (Article 32)	Access control, integrity, confidentiality, availability, encryption.

[48] Ibid.
[49] A Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (n 4).
[50] D Huth, F Matthes, 'Appropriate Technical and Organizational Measures: Identifying Privacy Engineering Approaches to Meet GDPR Requirements' (n 35).
[51] M Drev, B Delak, 'Conceptual Model of Privacy by Design' (n 10).

Transparency	Basic principles of the GDPR (Article 5), legality of processing (Article 6), notification of individuals (Article 12).	Processing transparency, responsibility.
Respect for the individual	Informing individuals (Article 12), rights of individuals (Articles 15, 16, 17, 18, 20, 21).	Processing transparency, responsibility

From the comparison table, it can be seen that the basic building blocks of privacy by design (except "full functionality") are present in all presented approaches (Table 3). A conceptual model of privacy by design could therefore be designed with the help of building blocks from any approach or with a combination of different approaches. However, when combining approaches, care must be taken to preserve elements from the same lines, as these refer to related concepts in terms of content, and it is also reasonable to determine the basic starting point, as there may be terminological ambiguities, duplication and the introduction of unnecessary complexity into model.

Elements from the GDPR framework were identified and used as building blocks for the conceptual model of privacy by design (Figure 1). They were grouped into one of three sets: "legal elements", "security elements", and "privacy by design and by default elements".[52] The sets are consistent with the structure of GDPR where legal elements occupy a central position, followed by data security, and finally by privacy by design and by default provisions.

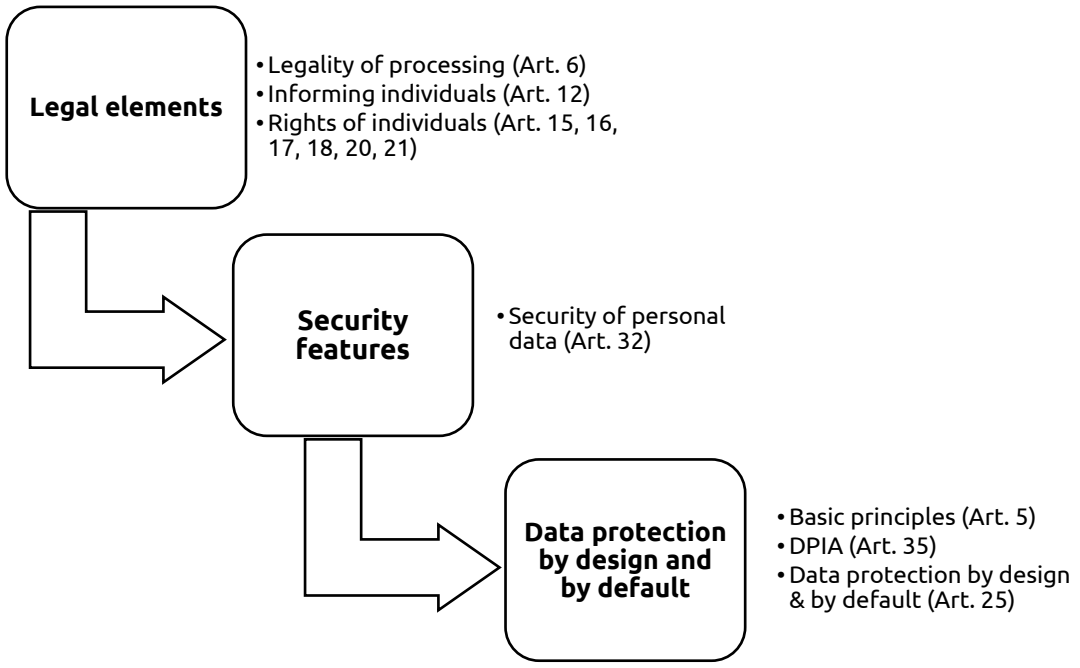


Figure 1: Representation of the conceptual model of privacy by design.[53]

[52] Ibid.
[53] Ibid.

The described conceptual model was tested on the Slovenian central health information system (eHealth) in 2021.[54] Two years later, the model was tested on three additional healthcare organizations, however, the results have not yet been published.

4. Discussion.

The fundamental question—whether one privacy by design framework offers noticeable advantages over others—remains unresolved. Currently, the available data is insufficient to provide a definitive answer. The comparison made in this article was theoretically oriented, however, the challenge of finding out if the specific framework is more effective in promoting theoretical understanding or providing the development of conceptual tools is beyond the scope of this article. This assessment may present a considerable test for future research attempts in the field.[55] It will require tackling difficult questions such as how to evaluate the effectiveness, how to compare different frameworks and models, and how to isolate the analyzed personal data processing operations in a way that will allow testing of different models without the intervention of one interfering with and skewing the results of another.[56] As the theoretical foundations of some of the privacy frameworks vary widely and are substantially different, it would be appropriate to compare those frameworks that display sufficient similarities in content and structure. Evaluation criteria could be developed using established standards, for example, ISO/IEC 27701 which deals with personal data protection.[57] Such a set of criteria could form the basis for a comprehensive assessment tool that can objectively measure each framework's proficiency. Case studies would then have to include organizations with comparable data processing complexities. Focusing on similar organizations could help control variables and improve the reliability of comparisons.

Regarding the work done with the conceptual model that was derived from the GDPR framework, the results are favorable for the time being. It seems that the model provides an appropriate compromise between generality and specificity.[58] However, one challenge lies in ensuring diversity within these studies. Namely, all four studies were made on organizations in the healthcare sector in one EU member state, therefore substantially different circumstances could open new dilemmas and show different results.[59] While promising, these findings may not extend to other areas or organizations with different levels of

[54] M Drev, D Stanimirović, B Delak, 'Implementation of Privacy by Design Model to an eHealth Information System' (n 11).
[55] O Ayalon, E Toch, 'User-centered privacy-by-design: Evaluating the appropriateness of design prototypes' (2021) 154 Int J Hum Comput Stud 102641.
[56] F Bu and others, '"Privacy by Design" implementation: Information system engineers' perspective' (2020) 53 Int J Inf Manage 102124.
[57] L Carmichael, W Hall, M Boniface, 'Personal data store ecosystems in health and social care' (2024) 12 Front Public Health 1348044.
[58] S Mohanty, 'Security and Privacy by Design is Key in the Internet of Everything (IoE) Era' (2020) 9(2) IEEE Consumer Electron Mag 4–5.
[59] A Carboni and others, 'Privacy by design in systems for assisted living, personalised care, and wellbeing: A stakeholder analysis' (2023) 4 Front Digit Health 934609.

data-processing complexity. Important consideration in evaluating privacy by design frameworks is the varying impact of sector-specific regulatory and operational requirements.[60] Different industries have unique data protection challenges and requirements, which can influence the relevance and effectiveness of specific privacy frameworks. For instance, healthcare organizations must adhere to strict data privacy standards due to the sensitive nature of health information, while financial institutions may focus more on data security due to the risk of financial fraud.[61] Understanding the sector-specific impact of privacy frameworks is essential for determining whether one framework is better suited for a particular type of organization over another. Therefore, future research should include a comparative study of privacy frameworks across sectors with distinct data handling conditions, regulatory requirements, and personal data processing complexities. This would reveal the adaptability and effectiveness of different privacy by design models in addressing diverse compliance landscapes and operational demands. Such research could also help organizations in specific sectors identify frameworks that best align with their privacy obligations and security goals.[62] Adding organizations from non-EU countries would also add to the diversity of the testing environment and in perspective enable higher robustness of the conceptual model. Such an expansion of the model could reveal different sector-specific challenges and insights that remain hidden within a single industry or region.[63] A promising venue for further research in this context would be comparing GDPR with other personal data protection Acts, most notably the Health Insurance Portability and Accountability Act (HIPPA)[64] and ADDPA.

In the long term, however, automated implementations—potentially through AI-based tools—could streamline the evaluation and integration of privacy frameworks across organizations. AI-driven analysis and automation could simplify the application of privacy by design principles, potentially offering solutions for real-time compliance and adaptive privacy strategies.

A successful implementation of any privacy by design framework hinges on effective stakeholder engagement, particularly from those responsible for data handling and privacy compliance within an organization.[65] Different frameworks may vary in how they encourage stakeholder involvement, training, and accountability, all of which are critical for effective privacy management. Therefore, future studies should evaluate how well various frameworks support stakeholder engagement and facilitate privacy-conscious

[60] L Iwaya and others, 'On the privacy of mental health apps: An empirical investigation and its implications for app development' (2023) 28(1) Empir Softw Eng 2.
[61] A Tewari, 'mHealth Systems Need a Privacy-by-Design Approach: Commentary on "Federated Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review"' (2023) 25 J Med Internet Res e46700.
[62] A Aljeraisy, M Barati, O Rana, C Perera, 'Privacy laws and privacy by design schemes for the internet of things: A developer's perspective' (2021) 54(5) ACM Computing Surveys (Csur) 1–38.
[63] E Schultes, M Roos, LO Bonino da Silva Santos, G Guizzardi, J Bouwman, T Hankemeier, A Baak, B Mons, 'FAIR Digital Twins for Data-Intensive Research' (2022) 5 Front Big Data 883341.
[64] A Oakley 'HIPAA, HIPPA, or HIPPO: What Really Is the Heath Insurance Portability and Accountability Act? ' (2023) 42(6) Biotechnology Law Report.
[65] L Alkhariji and others, 'Semantics-based privacy by design for Internet of Things applications' (2023) 138 Future Gener Comput Syst 280–295.

organizational cultures. For example, frameworks that mandate regular training, clear reporting channels, and contractual as well as accountability mechanisms may foster a stronger privacy culture than those lacking such requirements.[66] Additionally, engaging stakeholders early and often in the framework selection and implementation processes can ensure that privacy practices align with organizational values and practical needs.[67] This emphasis on stakeholder engagement can also influence the framework's long-term sustainability, as continuous involvement and feedback help refine privacy practices. Future studies could investigate the degree to which stakeholder engagement influences the overall effectiveness of privacy frameworks, which would provide valuable insights into best practices for fostering organizational commitment to privacy by design principles.

5. Conclusions.

From its origins in the 1990s, the idea of privacy by design has seen notable expansion. In addition to academic interest, it became part of the most comprehensive legal document for the protection of personal data – GDPR. Because of the increasing influence of ICT, (re)thinking privacy is becoming increasingly interesting for organizational and information science. With increasing risks of cybersecurity threats, integrating privacy measures such as data minimization, pseudonymization, and encryption, should also benefit the resilience of information systems without sacrificing general usability. Authors offered different frameworks for understanding privacy by design. A comparison of these approaches shows that commonalities are much more prevalent than differences. Such commonalities can be used to form common grounds for new ventures: from a deeper understanding of privacy to the development of conceptual tools and models which could even be integrated with artificial intelligence interfaces for more efficient (semi)automated implementation.

[66] E Tosi, 'Dati personali e contratto: un ossimoro apparente' (2023) 2 EJPLT 71–92.
[67] R Raab and others, 'Federated electronic health records for the European Health Data Space' (2023) 5(11) Lancet Digit Health e840–e847.

Angelini A, 'Neurotechnology in the research of evidence and in decision-making process: a dual perspective analysis' (2024) 2 EJPLT, 233 – 246.
DOI: https://doi.org/10.57230/EJPLT242AA

EJPLT
ISSN 2704-8012



Neurotechnology in the research of evidence and in decision-making process: a dual perspective analysis

Le neurotecnologie nella ricerca della prova e nei processi decisori: un'analisi a doppia prospettiva

ALICE ANGELINI
Ph.D. student in Criminal law
University of Insubria

Abstract

Neurotechnology in evidence collection and in decision-making must address the presumption of innocence and the prohibition of self-incrimination. The analysis adopts a dual approach: the philosophical perspective highlights the ethical dimension of free will, while the legal perspective addresses the technical aspect of protecting fundamental rights. Crucial safeguards include the inadmissibility of evidence obtained in violation of the self-incrimination prohibition and the evaluation of neurotechnological data as mere circumstantial evidence requiring corroboration.

L'uso delle neurotecnologie nella ricerca probatoria e nei processi decisori si scontra con la presunzione d'innocenza e il divieto di autoincriminazione. Il contributo affronta il tema da una duplice prospettiva: quella filosofica mette in luce la dimensione etica del libero arbitrio e quella legale la dimensione tecnica della tutela dei diritti fondamentali. Restano fondamentali le garanzie di inammissibilità delle prove ottenute in violazione del divieto di auto-incriminazione e la valutazione dei dati neurotecnologici come meri elementi di prova necessitanti corroboration.

© The author(s) 2024, 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: neurotechnology; criminal proceedings; research of evidence

Summary: 1. Introduction. – 2. Definitions. – 3. The philosophical perspective on free will. – 4. The legal perspective in the research of evidence. – 5. Neuroscientific tools and their Court admissibility. – 6. Constitutional principles and neurotechnologies. – 7. Neurotechnologies and sentencing disparity. – 8. Neurotechnology and human rights. – 9. Conclusions.

1. Introduction.

This paper pertains to the presentation of '*Neurotechnology in the research of evidence and in decision-making process: a dual perspective analysis*' at the Scuola Superiore S. Anna in Pisa during the conference '*Bridging the gap between neurorights and cyberights: introducing new ethical and legal safeguards for protecting humans in the digital era*'.

The discussion herein addresses the application of neurotechnology in legal proceedings for the collection of evidence, emphasizing the necessity of safeguarding the presumption of innocence and prohibiting self-incrimination. Additionally, it examines the role of neurotechnology as a tool within criminal policy.

The paper begins with definitions, in particular of the lexem 'criminal proceedings' and the term 'neurotechnology', exploring their interplay both in the evidence collection phase and the judicial decision-making process.

It then delves into the challenges posed by neurotechnology, particularly as it is increasingly used to assess 'mens rea'. This focus calls for a closer analysis of: a) the extent to which it can verify criminal intent, while evaluating the risks of infringing upon privacy and the right to self-defence and b) the potential for sentencing disparities between cases resolved with these tools and those adjudicated without them, particularly due to the economic constraints faced by defendants and issues related to the use of neurotechnological tools without respect for the right to counterproof.

The question described will be approached from a dual perspective: the philosophical perspective sheds light on the relationship with the ethical dimension of justice, while the legal perspective provides a bridge to its technical dimension. From the philosophical perspective, we will analyse the issue of free will to understand legal implications for the defendant's rights and moral freedom. The scientific literature presents a spectrum of positions, ranging from determinism to libertarian incompatibilism and compatibilism. Contemporary viewpoints, such as new compatibilism, underscore the importance of the perception of actions, positing that if persons perceive themselves to be acting freely and autonomously, they may be deemed responsible. These insights could facilitate ethical conclusions regarding the influence of neurotechnological elements on judicial decision-making, and the potential violations of defendants' rights by these tools. In essence, the inquiry revolves around how neurotechnology and legal proceedings may coexist while upholding human rights.

From the legal perspective, we will explore how neurotechnology can enhance evidence collection, in accordance with individual fundamental rights, and the implications for equity. This examination will involve analysing the procedural admissibility of neuroscientific evidence, using case law principles to provide additional insights. The criteria of reliability and falsifiability established by American jurisprudence in the Daubert standards are of paramount importance.

National Courts in Italy, from the lower Courts to the Court of Cassation, have scrutinized the advantages and disadvantages of neuroimaging and lie detection techniques as well as doctrinal studies focused on their impact on the principle of equity in decision-making. Nonetheless, uncertainties regarding the reliability of results, procedural risks, and potential overreliance on neuroscientific data during evidence collection persist. Additionally, the scientific challenge of reconciling emotional states with corresponding brain areas remains unresolved. On this field, the use of artificial intelligence in legal proceedings persists as an issue in background.

Finally, we will explore whether potential solutions could be identified through procedural safeguards, such as the inadmissibility of results or proceedings to obtain evidence that violate the prohibition against self-incrimination or the assessment of data as mere evidence requiring corroboration. However, the evolving nature of criminal law leaves the question open to further exploration.

2. Definitions.

Before examining how criminal procedure and neurotechnologies may intersect, it is crucial to define both concepts clearly.

It is essential, in fact, to clarify that the term 'proceedings' pertains specifically to the context of criminal procedure, with the purpose of analysing what kinds of intersections might exist between criminal proceedings and neurotechnologies.

Paolo Tonini defines *criminal procedure* as 'the legal process through which the state, acting through its judicial authorities, determines if a crime has been committed, identifies the person responsible, and applies the appropriate sanctions'.[1]

So, with the locution 'criminal proceedings', we intend a series of acts aimed at making a judicial decision, mainly based on the ascertainment of responsibility.

Neurotechnologies, according to Oliver Müller and Stefan Rotter, are an assembly of methods and instruments that enable a direct connection of technical components with the nervous system.[2] These technologies are utilized to enhance our understanding of brain function, treat neurological disorders, and improve human-machine interactions. Marcello Ienca

[1] P Tonini, *Manuale di procedura penale* (19th edn, Giuffrè 2018) 67.
[2] O Müller, S Rotter, 'Neurotechnology: current developments and ethical issues' (2017) 11(93) Frontiers in Systems Neuroscience, 1.

emphasizes that these technologies include brain-computer interfaces (BCIs), neuroprosthetics, and various forms of neural enhancement and stimulation.[3]

Neurotechnologies and legal proceedings come to represent links in the same chain when the former must enter the latter. This analysis will focus on the critical points of the intersection upon the introduction of neurotechnologies in the proceedings as evidence (i.e. admissibility of the evidence) and in the evaluative phase (i.e. as criminal policy tool).

In fact, the integration of neurotechnologies into the legal process raises significant philosophical, ethical, and legal issues, particularly concerning the determination of *mens rea* or criminal liability. These issues involve the protection of individual *moral freedom* and the principle of *equal treatment*.

In the following sections, we will examine the theoretical platforms of this problem from a philosophical perspective and from a legal perspective.

Philosophical and legal approaches are just some of the tools available to analyse the intersection between neurotechnology and process, as criminal law evolves in response to human evolution, technological innovation but must nevertheless preserve ethical and juridical safeguards and maintain and further promote the respect of human rights.

3. The philosophical perspective on free will.

In examining the philosophical perspectives regarding the existence or non-existence of free will, a debate has emerged within criminal law between those advocating for a rethinking of legal categories in light of neuroscientific contributions to the understanding of certain human behaviors,[4] and those who contend that philosophical inquiries can better explain some material phenomena without necessitating a radical overhaul of the criminal liability framework.[5] The latter, in fact, assert that criminal law categories constitute a shared linguistic code, pragmatically employed to provide a stable foundation for the entire criminal justice system, thereby ensuring a minimum level of equality and equal treatment.

The desire to redefine criminal law categories is primarily advocated by proponents of *philosophical determinism*. According to these scholars, [6] concepts like criminal liability and culpability, which presuppose that individuals act with full consciousness and volition, are untenable in light of the identity between mind and brain or at least the knowability of the mechanisms underpinning them. Consequently, this perspective negates the concept of free will, reducing freedom to a mere perception.

Conversely, *incompatibilist libertarians* assume that human action is based on metaphysical contra-causal freedom. A critique of the 'metaphysical' nature of their theories is articulated in a work by Mario Calderoni, who, as early as 1939, asserted that what matters is physical freedom, that is the ability of human

[3] M Ienca, 'Tra cervelli e macchine: riflessioni su neurotecnologie e su neurodiritti' (2019) Politeia, 60-61.
[4] L Santa Maria, 'Diritto penale sospeso tra neuroscienze ancor giovani e una metafisica troppo antica' [2017] DPC, 2.
[5] F Basile, G Vallar, 'Neuroscienze e diritto penale: le questioni sul tappeto' (2017) 4 DPC, 272-275.
[6] Santa Maria, 'Diritto penale' (n 4) 2.

beings to determine themselves and modify their actions based on foreseeable consequences.[7] In this regard, he was a precursor to compatibilist theses.

According to *compatibilist* doctrines, 'a person is free to do or not do what they want, but they are not free to will',[8] as individuals have no control over their mental states. Neuroimaging studies have shown that will emerges prior to the formation of consciousness, manifesting as an immediate reaction to impulses. From this, it follows that conscious will does not initiate actions but constitutes just one of the many links in the decision-making chain.

A more compelling theory appears to be that of the *new compatibilists*, who invoke the concept of perception.[9] They argue that the physical explanation of the extent to which human choices are free or constrained is irrelevant; what matters is human perception. If individuals perceive themselves to have acted freely, with consciousness and volition – regardless of whether these perceptions are merely illusory – then it becomes possible to attribute responsibility to them.

Although the theories of new compatibilism seem particularly acceptable even from a criminal law perspective, the issue of responsibility should remain entirely separate from the philosophical or scientific explanation surrounding the nature of will. *Responsibility* is a shared concept, essential for regulating behaviour at the social level, and should not be influenced by philosophical explanations regarding the degree to which will is shaped by genetic or environmental factors.[10]

These considerations, however, resurface when evaluating the admissibility of neuroscientific evidence, given its capacity to probe the human mind through techniques that profoundly penetrate its workings.

4. The legal perspective in the research of evidence.

Building upon this philosophical platform, we now turn to the legal perspective on neurotechnologies, which involves the interaction of neuroimaging tools in legal proceedings. The issue concerning the interaction between neurotechnologies and process arises from the assumption that human behaviour is, to some extent, predetermined and that the causes of actions are knowable if scientifically explained. This assumption has facilitated the introduction of neuroscience into the criminal process, albeit at an embryonic and sporadic level.

However, until the early 1990s, the use of neuroscience as a means of evidence was not regulated. Questions emerged regarding whether it represented a method for researching typical or atypical evidence and what procedural framework, as well as its implications, it should entail.

---

[7] M Calderoni, *I postulati della scienza positiva* (G Ramella e C 1901), 39-43.

[8] MB Magro, 'Le mille porte del libero arbitrio: compatibilismo e epifenomenalismo secondo le neuroscienze' (2020) 2 Riv It Med Leg, 717.

[9] Ibid 724-726.

[10] This is also based on Calderoni's teachings, which emphasize the need to keep the concept of responsibility separate from philosophical explanations of free will. For further reference, see M Calderoni, *I postulati della scienza positiva* (n 7) 43.

American jurisprudence has only recently solidified a response to this issue through the establishment of the *Daubert criteria* concerning the admissibility of scientific evidence in court, which superseded the 1923 *Frye ruling*.

While the Frye decision established that the criterion for admissibility of evidence was the 'general acceptance by the relevant scientific community', the Daubert ruling of 1993 must contend with a peculiar characteristic of neuroscientific evidence, namely the often-unsatisfactory levels of reliability of scientific data. Given that the methodologies were limited and rarely achieved the threshold of general acceptance, the Daubert criteria introduced additional requirements, including the testability and falsifiability of the method, subjecting the evidence to peer review, ensuring the independence of the expert, and explicitly stating the error rate.

These criteria were subsequently incorporated and further refined within the national context in 2010 by the *Cozzini ruling*,[11] which particularly emphasizes two aspects: the authority of the expert and the necessity for the expert to bear the burden of presenting to the judge a comprehensive range of opinions from the scientific theories pertaining to the methods in question. This approach seeks to provide the judge with a holistic overview of the available options. Consequently, judges are required to verify a minimum threshold of reliability of neuroscientific data for the purposes of admissibility.

Despite the established principles enshrined in the Daubert-Cozzini criteria, legal scholarship continues to scrutinize the procedural use of neuroscientific data as a tool for investigating the psychological element of the crime and the boundaries of procedural admissibility. This scrutiny arises particularly in light of skepticism expressed in certain case law decisions regarding the matter, as well as concerns about potential infringement upon the rights of the defence and the conflicts with the prohibition of self-incrimination that these tools may engender.

5. Neuroscientific tools and their Court admissibility.

At this stage, it is necessary to consider which forms of neuroscientific evidence are likely to be admitted in court and what the associated challenges may be.

The latest legal scholarship[12] distinguishes between two categories: a) instruments investigating *individuals as sources of real evidence*, providing scientifically verifiable data freely appreciated by the judge and b) instruments *validating declarative evidence*, aimed at assessing the truthfulness of statements made by the defendant, witnesses, or victims.

a) The first category includes techniques such as Functional Magnetic Resonance Imaging (fMRI), brain fingerprinting, Computerized Axial Tomography (CAT scans), as well as Physical Biometric Applications (PBA) and

[11] Cass sez IV pen, Sept 17, 2010, n 43786 (Cozzini et al.)

[12] MR Anglani, 'Neurolaw: l'incidenza delle neuroscienze sugli standard del processo penale e sulla «libertà morale della persona»' (2024) 6 federalismi.it, 57-58.

Behavioral Biometric Applications (BBA).[13] These instruments are used to determine whether the subjects exhibit brain damage or physically detectable pathologies, aiding in the evaluation of culpability.

b) The second category consists of lie and memory detection tools, such as fMRI, the Implicit Association Test (IAT), the Autobiographical Implicit Association Test (A-IAT), and the Timed Antagonistic Response Alethiometer (TARA). These instruments evaluate the truthfulness of statements by analysing physiological reactions, such as blood flow measurements, response times, and associative links.

While the first set of tools generally raises no concerns regarding moral autonomy – since they provide objective, scientifically measurable data and may be admissible even without the defendant's consent, given that dignity is respected in the collection of such data – the second set presents significant concerns in terms of potential conflict with the principle against self-incrimination.

However, several considerations must be taken into account.

1) Functional MRI, like others lie detection methods, detects increased blood flow in the brain during emotional responses. However, human *reactions vary widely*. Factors such as learned deception or neurological conditions can influence these responses, complicating their interpretation. The detection may also vary in the presence of childhood traumas or brain diseases, which alter the intensity of blood flow, adding another layer of complexity.[14]
2) Neurotechnologies run the risk of reducing individuals to *mere data points*, potentially undermining core elements of personal identity, awareness and self-determination.[15] Concerns about 'brain hacking' also arise,[16] though a detailed discussion on this matter is beyond the scope of this paper.
3) The use of neurotechnologies to assess subjective states may conflict with the principle of *moral freedom* in testimony, as culpability is typically tied to external, observable actions rather than internal mental states. In this regard, it is worth recalling the Raso ruling (2005), which included personality disorders within the legal concept of infirmity, as such disorders can affect the judgment of culpability.[17]

Another part of legal scholarship[18] distinguishes between *invasive methods* (such as DNA or genetic sampling, CAT scans, PET scans) and *non-invasive methods* (e.g. lie or memory detection).

With regard to invasive methods, legal scholars have stated that if neurotechnological assessments involve a *pati* (e.g., passively providing a

[13] GJ Sicignano, 'Brief reflections on the role of forensic evidence in the Italian criminal justice system' (2023) 1 *EJPLT*, 125-126.
[14] L Bain and others, *Neuroforensics. Exploring the legal implications of emerging neurotechnologies. Proceedings of a workshop* (The national academic press 2018), 13-14.
[15] G Gulotta, M Caponi Beltramo, 'Neurodiritti: tra tutela e responsabilità' [2021] Sistema Penale, 1.
[16] For further reference, please refer to G Gulotta, M Caponi Beltramo 'Neurodiritti' (n 15) 5.
[17] Cass pen, Sez Un, Jan 25, 2005, n 9163 (sentenza Raso); A Santosuosso, B Bottalico, 'Neuroscience and behavioral genetics in the italian criminal proceedings. Cases and perspectives' (2013) 1 Rassegna Italiana di Criminologia, 72-74.
[18] S Ruggeri, 'Neurosciences, criminal justice and individual safeguards' (2023) 2 Processo penale e giustizia, 287-288.

biological sample), they are permissible and do not violate the principle against self-incrimination.[19] However, if these assessments require active participation or communication without consent, they infringe upon the *nemo tenetur se detegere* principle, as involuntary statements breach the right to remain silent. Thus, the Court upholds the principle of the privilege against self-incrimination.

Similarly, if lie and memory detection tools were coercible, they would violate the principle of *nemo tenetur se detegere*.

In particular, the Implicit Association Test (IAT) raises concerns about self-determination, as it investigates memory, which is susceptible to alteration, rather than facts.[20] Therefore, results from the IAT must be corroborated through adversarial proceedings, as the test alone cannot constitute conclusive evidence but should be considered as a clue.

Finally, all neuroscientific tools elicit concerns about their reliability. Despite the Daubert criteria, which entrust judge as *peritum peritorum*, who must evaluate evidence according to their expertise, the overall reliability of scientific evidence remains relatively low.

This brings us to further challenges regarding the neurotechnological assessments on the functions of punishment. These tools potentially conflict with the principle of culpability and rehabilitation, since a conviction based on uncertain data does not allow the convict (possibly innocent) to understand the wrongdoing's disvalue.

6. Constitutional principles and neurotechnologies.

To address these issues, it is essential to rely on fundamental principles. In this paragraph, we will analyse how the challenges presented by neurotechnologies should be addressed in light of the Italian Constitution.

First and foremost, the question arises as to how these challenges can be reconciled with the right to defence, as enshrined in Article 24 of the Constitution, and the right to evidence under Article 111 of the Constitution.[21]

These two principles stand in contrast to the right to health, articulated in Article 32 of the Constitution, which states that 'no one can be obliged to undergo specific health treatment except by law' and to the principle of *nemo tenetur se detegere*, also contained in Article 24 and included in the Code of Criminal Procedure.

Secondly, it is necessary to clarify the legality and limitations of consent to neuroscientific assessments.

Our criminal justice system upholds the principle of freedom of self-determination, as outlined in Article 188 of the Code of Criminal Procedure, which prohibits methods or techniques that influence self-determination or alter the ability to recall or evaluate facts.

[19] S Ruggeri, 'Neurosciences' (n 18) 286.
[20] FR Dinacci, 'Neuroscience and criminal trial: probatory reasoning between evaluation chemistry and rational logic' (2016) 2 Processo penale e giustizia, 7.
[21] FG Pizzetti, 'La Costituzione e l'uso in sede giudiziaria delle neuroscienze (e dell'intelligenza artificiale): spunti di riflessione' (2019) 2 Biolaw journal, 702.

Two court rulings exemplify this balance:[22] the Court of Appeal of Salerno (2575/2016)[23] prohibited techniques that influence self-determination, even with consent, asserting that information must be collected externally; and the Court of Appeal of Brescia (1683/2020)[24] ruled that the IAT test contradicts Article 188, affirming that self-determination and moral freedom are indispensable rights.

There are diverging views on these matters. Some argue that this conflicts with the right to evidence under Article 111; while others maintain that neuroscientific tools should require counterevidence.[25] Some accept them but acknowledge critical issues.[26]

Some others, finally, argue that lie or memory detection tools are inadmissible only if imposed by the prosecutor or judge; however, if the defendant voluntarily submits to them, there is no violation, as no recognized right exists to 'not to be discovered of lying'.[27]

Nonetheless, the constitutional protection against self-incrimination and the right to moral freedom are broader in scope.

Assuming neurosciences as typical evidence with atypical content – though this aspect will not be elaborated here[28] – Article 189 of the Code of Criminal Procedure on atypical evidence mandates that evidence must be suitable for determining the facts and for protecting moral freedom. Corda suggests a 'variable intensity' for the criterion of suitability, which is more flexible when applied to the defence, with the aim of raising reasonable doubt rather than persuading. This preference supports admissibility.[29]

Based on this premise, it must be asserted that using techniques on the subject as evidence is permissible where it does not affect self-determination and results are used only *in favor rei* (not as incriminating evidence).

Indeed, the issue must be resolved through the principle of *favor rei* and the proper application of the beyond reasonable doubt (BARD) standard.

We need to address this issue on two levels.

a) When is it truly necessary to rely on neurotechnological tools?

Neurotechnological tools are certainly essential for assessing physical impairments, especially to prevent the conviction of individuals who are legally non-chargeable. However, there is no need to investigate the truthfulness of the defendant's statements (and their internal forum), as this would violate the prohibition against using methods that influence self-determination.

The real risk, however, arises when the defence voluntarily employs neuroscientific tools to seek favourable evidence, but obtains unfavourable results. In such cases, it is crucial to determine whether these results stem from the dishonesty of the defendant or from a flaw in the tool itself. If dishonesty

[22] F Cirillo, 'Neurodiritti: ambiguità della 'libertà cognitiva' e prospettive di tutela' (2023) II Consulta Online, 682-686.
[23] Court of Appeal of Salerno, Dec 16, 2016, n 2575.
[24] Court of Appeal of Brescia, July 15, 2020, n 1683.
[25] F Cirillo, 'Neurodiritti' (n 22) 683.
[26] O Di Giovine, 'Prove di dialogo tra neuroscienze e diritto penale' (2016) 4 Giornale italiano di psicologia, 336.
[27] S Ruggeri, 'Neurosciences' (n 18) 291.
[28] Reference is made in greater detail to A Corda, 'Neuroscienze forensi e giustizia penale tra diritto e prova (Disorientamenti giurisprudenziali e questioni aperte)' (2014) 3 Archivio penale, 27.
[29] ibid 27.

is involved, it must be determined whether the initial consent for the assessment also covers results that are against the defendant.

Conversely, if a defect in the tool is identified, its functionality should be evaluated through *expert comparisons* among individuals with technical expertise, such as doctors, psychologists, technicians who designed the tool, and legal counsel.

b) What is the solution if lie or memory detection tools are the only means to prove innocence?

In such cases, the necessity arises from a history of improper use of the *BARD standard*: a conviction should only be pronounced when there is unequivocal certainty, following the criterion that it is better for a guilty person to go free than for an innocent person to be wrongly convicted'. However, given the difficulty of refining the BARD standard without altering judicial practices potential solution could be to render lie or memory detection tools inadmissible when used *contra reum* and allowing their use solely *in favor rei*.

Thus, the cautious use of minimally invasive neuroscientific tools becomes compatible with the preservation of moral freedom, provided that the data obtained are considered inadmissible if used *contra reum*, both at the time of acquisition and at the time of judgment (where such evidence should not prevail).[30]

However, if moral freedom were elevated to an absolute principle, what would this affect the rights to health, defence and evidence?

The use of truth-finding measures is therefore permissible under the following conditions:

1) the defendant has given explicit consent;
2) the technique is minimally invasive;
3) the underlying theories are widely recognized and credible;[31]
4) it is the only available means for the defendant to prove his/her innocence;
5) the evidence is rendered inadmissible if it is unfavourable to the defendant.

On the other hand, sacrificing the defendant 'in the name of his moral freedom'[32] is not acceptable.

An additional observation must be made regarding the admissibility of neuroscientific evidence under the aforementioned conditions. It is indeed possible that evidence favorable to the defendant for the purpose of determining guilt may still prove decisive in an unfavourable sense, specifically in assessing dangerousness and, consequently, in the imposition of security measures. If, in fact, neuroscientific evidence was to demonstrate the subject's partial or total incapacity, it must also be considered that such data could be interpreted as an indicator of the subject's dangerousness and may, therefore, serves as basis for the imposition of a security measure.

In this regard, the procedural use of neurotechnologies could, in fact, consistently result in unfavorable outcomes for the defendant.

[30] AU Palma, 'Le "prove di verità" e la libertà morale del dichiarante' (2020) 1 Archivio Penale, 51.
[31] These first three conditions were identified by A U Palma in 'Le "prove di verità"' (n 30) 55.
[32] ibid 56.

7. Neurotechnologies and sentencing disparity.

Finally, it is necessary to reflect on the judge's evaluation of neurotechnologies as evidence and the potential for sentencing disparity.

The issue arises when considering the principle of equal treatment in two different concrete situations: a) between cases in which neuroscientific tools are employed and those in which they are not; b) in cases in which neuroscientific tools are employed exclusively on the victim of the crime.

a) Regarding the first issue, a pertinent example can be drawn from the case of Como (G.i.p. Como, 2011)[33]. In this case, the perpetrator not only killed her parents but also, during the investigation, her sister to secure the inheritance.

Her stated intention conflicted with her actual motive, which prompted a psychiatric evaluation during the trial, but the psychiatric assessment yielded conflicting results.

The defence then sought to conduct a functional MRI (fMRI) on the woman to demonstrate the presence of a mental disorder, which, when corroborated with other findings, led the court to recognize a partial mental incapacity. Based on the initial evaluation, a conviction would likely have been reached, but it was only with the use of neuroscience that partial incapacity established.

It is important to reflect on what might have occurred if the defence had not chosen to rely on neuroscientific tools.

In some cases, neuroscientific evidence can shift the balance *in favor rei*, leading to a declaration of partial or total incapacity (with the previously discussed limits).

It is therefore necessary to consider what happens in cases where these techniques are not utilized.

It can be argued that the defence's decision to use neuroscientific evidence becomes a determining factor, with the risk that neuroscientific tools, given their cost, are more accessible to wealthier individuals. This disparity calls into question the egalitarian nature of justice.[34]

b) Concerning the potential risks associated with employing neuroscientific tools on the injured party, the Cremona case (G.i.p. Cremona, 2011)[35] serves as useful reference. In this instance, the defendant was accused of sexual harassment with abuse of authority. Due to conflicting statements from both parties and witnesses during the trial, the judge ordered a neuroscientific examination to verify whether the victim had a memory of the alleged harassment.

The IAT test was utilized, confirming the allegation, and the defendant was convicted based on the neuroscientific expertise conducted solely on the statements of the victim, which represents a *privileged evidence*.[36]

In this scenario, the conviction was based on unfavourable neuroscientific evidence obtained without the defendant's consent and without granting them the right to present counterevidence.

---

[33] Trib Como, G.i.p., May 20, 2011.
[34] G Gulotta, M Caponi Beltramo, 'Neurodiritti' (n 15) 8.
[35] Trib Cremona, G.i.p., Jul 19, 2011, n 109.
[36] FR Dinacci, 'Neuroscience and criminal trial' (n 20) 8-9.

This case illustrates that the exclusive use of neuroscientific tools on the victim may entail a latent risk, as it could skew the judgment *contra reum*, relying solely on the victim's memories – or, more precisely, on what the victim believes to remember.

When employing neuroscientific tools on the victim, it is advisable for the neuroscientific evidence to be deemed valid only if acquired under the same conditions for the defendant as well. Otherwise, there exists a risk of infringing upon the defendant's right to defence – particularly the right to present counterevidence – as well as their right to self-determination.

From these two cases, it can be deduced that safeguards against such inequalities may lie in the principle of *adversarial proceedings*[37] and in the duty to *provide justification* for sentencing decisions.

Scientific evidence, in fact, must be subject to adversarial examination and evaluated alongside other forms of evidence, as affirmed in the *Franzese ruling*, [38] applying the criterion of logical probability. Judicial decisions, therefore, should take into account all the evidence gathered and cannot rely solely on neuroscientific data.

The duty to provide reasons for sentencing decisions requires judges to justify their conclusions based on all available evidence, articulating the logical reasoning behind their decisions. This justification must be particularly rigorous when largely based on neuroscientific data, emphasizing the unreliability of all exculpatory elements and clearly explaining the reasons for considering the neuroscientific evidence as credible, in order to avoid an over-reliance on such data.[39]

Di Chiara has issued a cautionary note regarding neurotechnologies, likening them to the sirens' songs or to the wax wings of Icarus and Daedalus in their attempt to escape the labyrinth.

Regarding the relationship between neurotechnologies and the judiciary, he observed that judges 'are not gods and yet they are equally dangerous like the ancient gods', in our view, particularly when they allow themselves to be swayed by neuroscientific data without critical examination.[40]

8. Neurotechnology and human rights.

Additional considerations could explore the use of artificial intelligence-based tools in both the research of evidence and the decision-making process,[41]

---

[37] ibid 9.

[38] F Fuscaldo, 'Il neuroimaging funzionale per l'analisi della prova dichiarativa' [2023] quotidianolegale.it.

[39] A common risk is the tendency to intuitively find reconstructions of facts based on neuroscientific information more convincing than those lacking such data, even when the neuroscientific evidence presented is irrelevant or incorrect, in DS Weisberg and others, 'The Seductive Allure of Neuroscience Explanations' (2008) 20(3) Journal of Cognitive Neuroscience, 470.

[40] G Di Chiara, 'Il canto delle sirene. Processo penale e modernità scientifico-tecnologica: prova dichiarativa e diagnostica della verità' [2007] Criminalia, 39.

[41] For an overview of the primary references, see S Quattrocolo, 'Equità del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo' (2019) 1 Revista Ítalo-Española de Derecho Procesal, 107-123; S Quattrocolo, 'Processo penale e rivoluzione digitale: da ossimoro a endiadi?' (2020) Media Laws, 121-135; V Manes, 'L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia' [2020] Discrimen; J Nieva Fenoll, *Intelligenza artificiale e processo* (Giappichelli 2019).

particularly as instruments grounded in a neurotechnological framework. However, such an analysis would open avenues that extend beyond the scope of this discussion.

An international overview on how human rights intersect with criminal proceedings is necessary.

Two main theories regarding human rights and neurotechnology can be identified.

According to the first theoretical approach, the existing legal framework is considered adequate to address the challenges posed by neurotechnologies in criminal proceedings.[42]

Conversely, the second approach advocates for the recognition of four new rights, collectively referred to as 'neurorights',[43] (right to cognitive liberty, right to mental privacy, right to mental integrity, right to psychological continuity).

In the context of criminal procedure, these rights serve specific purposes:

- the right to cognitive liberty ensures control over the application of neurocognitive technologies;
- the right to mental privacy protects against intrusive techniques, such as mental decoding, that could infringe upon a defendant's private sphere;
- the right to mental integrity prevents subjects from being exposed to invasive or harmful neurotechnological interventions without consent;
- the right to psychological continuity ensures that individuals' memory or identity is not unduly alterated during legal proceedings.

The challenge lies in reconciling these rights with the pursuit of procedural truth within judicial proceedings.

Alternatively, if we recognize that the creation of new rights is unnecessary, those already existent – such as physical or mental integrity, privacy and freedom of thought – might already provide sufficient protection against the coercive use of neurotechnologies, if they are adapted to the new challenges posed by these technologies.[44]

In light of these premises, memory and lie-detection tools present significant risks to the protection of these rights,[45] raising ethical concerns that also intersect with the application of artificial intelligence in legal contexts.[46]

---

[42] See C Bublitz, 'Neurotechnologies and human rights: restating and reaffirming the multi-layered protection of the person' (2024) 28(5) The international journal of human rights, 782-807, where the author argues that there is no need to establish new rights to address issues arising in criminal proceedings, as existing rights already provide protection against the misuse of neurotechnologies, though they would need to be further articulated to be applied to new scenarios.

[43] See M Ienca, R Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' (2017) 13(5) Life Sciences, Society and Policy.

[44] See C Bublitz, 'Neurotechnologies and human rights' (n 42) 783.

[45] An illustrative example of these risks, specifically related to the sentencing phase, is the *Wisconsin v. Eric L. Loomis* case, in which the defendant was evaluated using the COMPAS algorithm. It was later shown that the algorithm exhibited *racial bias.* Rather than establishing a direct causal link between the defendant's actions and the occurrence of the event, the algorithm, in cases of insufficient evidence, sought to base the determination of guilt on psychological assessments. See F Basile, 'Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine' (2019) 10 DPU.

[46] For a reflection on ethical implication in using AI tools, see JA Searle, *Intelligenza artificiale e Pensiero umano – Filosofia per un tempo nuovo* (Castelvecchi 2023); L Floridi, *Etica dell'intelligenza artificiale – Sviluppi, opportunità, sfide* (Raffaello Cortina Editore 2022).

The solution likely lies in striking a nuanced balance between procedural needs – such as the pursuit of trial truth – and the protection of human rights as a whole. This equilibrium can be upheld in criminal proceedings through established principles such as the right to self-defence, the right against self-incrimination and the principle of consent.

At this juncture, ensuring the adequate protection of human rights in the context of criminal proceedings remains an open question, demanding ongoing scrutiny, careful case-by-case adjudication and the evolving interpretation of case law.

9. Conclusions.

In light of the challenges posed by neurotechnologies as a source of evidence and their complex role in the decision-making process, we may conclude that, despite the criticisms, they represent a reality that cannot be ignored or underestimated, particularly given the increasingly pervasive nature of technological advancement.

New challenges also emerge with the development of Brain-Computer Interfaces (BCI), Deep Brain Stimulation (DBS) and closed-loop systems, commonly used as interfaces by individuals with disabilities. These technologies enable direct communication between the brain and an external device or allow external influence on the brain by using electrical impulses to stimulate specific areas once their characteristics have been mapped.

Such systems not only receive signals but also transmit them to the brain, with the potential to alter memories or, more broadly, the physical or psychological data may be investigated through the device itself, even though such techniques are currently restricted to therapeutic use.

The issue becomes more complex if these technologies are introduced in legal proceedings or if the individual undergoing the neuroscientific assessment is one who has been treated with such tools.

Finally, these tools test the boundaries of freedom of thought and pose significant questions about the ethical limits within which neuroscience may operate as a means of investigating the human mind.

As technology advances far more rapidly than the law, the key challenge lies in integrating these innovations while ensuring the protection of fundamental human rights.

Perilla Granados JSA, 'Plataforma europea de Resolución de Litigios en Línea (RLL): ecosistema digital en vía de extinción' (2024) 2 EJPLT, 247 – 260.
DOI: https://doi.org/10.57230/EJPLT242JSAPG

EJPLT
ISSN 2704-8012



Plataforma europea de Resolución de Litigios en Línea (RLL): ecosistema digital en vía de extinción

European Online Dispute Resolution Platform (ODP): digital ecosystem on the verge of extinction

JUAN SEBASTIÁN ALEJANDRO PERILLA GRANADOS
Associate Professor
Universidad Tecnológica de Bolívar

Abstract

A través del Reglamento (UE) 3228/2024 del Parlamento Europeo y Consejo se derogó el Reglamento (UE) 524/2013 y se modificaron los Reglamentos (UE) 2394/2017 y (UE) 1724/2018 para la supresión del ecosistema digital de Resolución de Litigios en Línea (RLL), el cual tenía tres funcionalidades principales: informar acerca de los alcances jurídicos del derecho del consumo, facilitar canales de comunicación directos para la gestión de disputas de forma directa y sugerir vías de solución de conflictos cuando la auto composición no es posible. Esta decisión responde a que se trataba de un diseño formalista con múltiples cuestionamientos antiformalistas. Entre otras razones, se evidenció que este ecosistema digital no materializa los derechos de los consumidores a plenitud, lo cual es sistematizado en el presente artículo con un enfoque hermenéutico crítico fundamentado en métodos cualitativos.

© The author(s) 2024, 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
Through Regulation (EU) 3228/2024 of the European Parliament and Council, Regulation (EU) 524/2013 was repealed and Regulations (EU) 2394/2017 and (EU) 1724/2018 were modified for the suppression of the digital ecosystem of Online Dispute Resolution (OLR), which had three main functionalities: informing about the legal scope of consumer law, facilitating channels direct communication channels to manage disputes directly and suggest ways to resolve conflicts when self-composition is not possible. This decision responds to the fact that it was a formalist design with multiple anti-formalist questions. Among other reasons, it was evident that this digital ecosystem does not fully materialize consumer rights, which is systematized in this article with a critical hermeneutical approach based on qualitative methods.

Keywords: Online Dispute Resolution; Digital Ecosystem; Conflict Management; Consumer Law; Contractual relationships

Summary: 1. Introducción. – 2. Funcionalidades de la plataforma digital RLL de la Comisión Europea desde el formalismo. – 3. Análisis antiformalista de las funcionalidades de RLL desde los derechos del consumidor. – 4. Conclusiones.

1. Introducción.

El contexto de la Unión Europea es considerado a nivel global como uno de los más robustos en asuntos referentes al derecho del consumo, lo cual se justifica al considerar que desde el nivel normativo se ha dado una protección reforzada a quienes ostentan un rol subordinado en los negocios del mercado[1]. Así, existen normas jurídicas organizadas por áreas, procurando agotar en la mayor medida posible las variables fácticas en las cuales se pueda presentar un problema entre un consumidor y un comerciante[2]. De esta manera, desde una perspectiva formalista, se considera que la positivización de normas jurídicas a través de medios escritos puede generar impactos concretos en la realidad para la cual se dirigen[3]. Se trata de un enfoque jurídico formalista, que ha permitido consolidar desde el derecho sustancial el reconocimiento de derechos y deberes tendientes a ser aplicados más allá de las particularidades de cada uno de los países europeos que las suscriben.

Ahora bien, el contexto de producción normativo de la Unión Europea es consciente que parte de esas normas jurídicas requieren de rutas procesales para que sea posible ejercer los derechos y exigir el cumplimiento de los

[1] El derecho del consumo gestado desde la Unión Europea se ha consolidado como referente trasnacional en contextos como el latinoamericano, lo cual es explicado en resultados de investigación como el siguiente: S Camargo, 'Los derechos del consumidor desde una perspectiva constitucional y de Derechos Humanos' (2022) 12 Rev.ces derecho, 146-161.

[2] Es posible comprender desde el contexto italiano los alcances que desde la Unión Europea se han dado al derecho del consumo, según se evidencia a continuación: S Pagliantini, 'Una mirada a la protección contractual del consumidor en Italia' (2015) 28 derpri, 191-200. Por su parte, es posible profundizar en estrategias procesales concretas a continuación: A. Sardu, 'La strategia di opposizione dell'Unione Europea all'arbitrato internazionale degli investimenti derivante da TBI intraunionali' (2019) 4 DPCE Online, 1-18.

[3] Los debates en torno al formalismo aplicado a áreas jurídicas específicas puede ser profundizado en este artículo científico: J Perilla, 'Construcción antiformalista del consumidor medio' (2015) 54 Rev. Derecho priv., 1-23.

deberes[4]. Así, la Comisión Europea consolidó una herramienta tecnológica para gestionar los conflictos entre consumidores y comerciantes, con el fin de permitir comunicaciones directas que procurasen aportar a la solución de las problemáticas que se pudiesen llegar a presentar[5]. Una de estas herramientas ha sido la plataforma europea de Resolución de Litigios en Línea (RLL), la cual contuvo, desde el momento de su creación, información para orientar a cualquiera de las partes en conflicto, pretendió generar canales de comunicación para poder acudir a los mecanismos alternativos de solución de conflictos y llegó a sugerir rutas adicionales en caso en que no fuese posible resolver las controversias con el uso de la plataforma[6]. Desde su creación, fue posible acceder a esta plataforma de manera gratuita y a través de la red de Internet sin ningún tipo de restricción, contando con lenguaje considerado por sus creadores como claro para la comprensión de sus contenidos.

Debido a estas múltiples funcionalidades y facilidades de acceso, esta plataforma digital contó con eficacia simbólica en el contexto europeo[7]. Esto significa que tanto consumidores como comerciantes conocieron de su existencia, al tiempo que comprendieron los beneficios, por lo menos en abstracto, que se pueden alcanzar con su utilización. Para efectos del presente artículo resulta especialmente relevante considerar la funcionalidad que tuvo en torno al inicio de la gestión de un conflicto y que sugiere la posibilidad que la parte alegante pueda contactar a su contraparte con el fin de procurar una solución de los conflictos. Se trató de una forma de dar protagonismo a las partes en pugna, para que pudiesen tener canales directos de comunicación y acordasen cuál era la mejor manera de solucionar sus problemáticas en tiempo relativamente cortos de treinta (30) días[8]. Así, se esperaba que el acceso a la

[4] Como un marco hermenéutico trasnacional para la comprensión de los debates en torno a la garantía de los derechos se recomienda consultar: J Cassagne, 'Los nuevos derechos y garantías' (2016) 3 Revista de Investigações Constitucionais, 59-108. Además, es posible considerar este referente: L. Gatt, 'Consumers and Digital environments as a Structural Vulnerability Relationship' (2022) 2022/2 EJPLT, 8-16.

[5] Sobre los desarrollos tecnológicos para la solución de controversias se puede consultar la siguiente investigación aplicada directamente a RLL: F Barrientos, 'Nuevas tecnologías para el acceso a la justicia del consumidor: Diagnóstico de la situación fragmentada en Chile y una propuesta a la luz de la plataforma europea online de resolución de conflictos' (2023) 12 Rev. chil. derecho tecnol., 1-36. Adicionalmente, se recomienda analizar estos debates tecnológicos desde una perspectiva aplicada en esta publicación: M. Gaeta, 'Green and Sustainable Mobility in Road Transport. How Private Law Can Guarantee the Right Balance Between Environmentally Sustainable Development and Digital Transformation' (2023) 34 European Business Law Review, 63-80.

[6] El modelo europeo ha sido analizado desde diferentes perspectivas académicas, ponderándolo como un avance significativo desde el RLL y esto se evidencia en este tipo de publicaciones: S Díaz, 'Análisis de los sistemas de solución de conflictos en línea en el mundo y propuesta para su implementación en Colombia' (2022) 11 Rev. chil. derecho tecnol., 245-276. Estos debates pueden ser analizados de forma aplicada en esta investigación: L. Gatt (2023), 'Responsabilità civile e diritto internazionale privato: un caso di studio' (2023) 4 ASSICURAZIONI, 27-74.

[7] La eficacia simbólica puede entenderse como la capacidad de las normas jurídicas, las instituciones legales y los actos de autoridad para influir en las creencias, valores y comportamientos de los individuos y de la sociedad a través de su poder simbólico, más allá de su aplicación estrictamente material. Esta dimensión simbólica del derecho no solo se refiere a la efectividad práctica de las leyes, sino también a cómo estas son percibidas, aceptadas o internalizadas por los sujetos. El concepto de eficacia simbólica que se adopta en este artículo responde a los lineamientos incluidos en la siguiente publicación: J Perilla, 'El Estado retado desde el constructivismo antiformalista: legitimidad y convicción' (2021) 14 Criterios, 21-36.

[8] Al respecto de la solución de conflictos a través de RLL se sugiere consultar: G Prado, 'La efectiva protección de los consumidores. Un nuevo aporte del Tribunal de Justicia de la Unión Europea a la integración europea' (2020) 52 Estud. int., 159-177. Por su parte, el estudio del derecho del consumidor en contextos europeos específicos puede ser analizado en esta investigación: S. Ghionzoli, 'The evolution of relationships between the customer and their bank, from the rules on transparency to the regulation on

solución de conflictos fuese directa, breve y coherente con los lineamientos normativos de la Comunidad Europea.

Y aunque las bondades de este aplicativo llegaron a considerarse como sobresalientes en el momento de su creación, se consolidaron críticas en torno a si las funcionalidades para la solución de conflictos sí materializa los derechos de los consumidores según la motivación que dio lugar a su creación[9]. Así, se concluyó que la plataforma, operativa desde 2016, ha tenido un bajo impacto, gestionando menos del 2% de los casos a ella presentados en un elevado tráfico[10]. evidenciando que el diseño formalista no cumple en la práctica con los fines pretendidos y que el rendimiento de la plataforma no justifica los costes asociados [11]. En consecuencia, a través del Reglamento (UE) 3228/2024 del Parlamento Europeo y Consejo se derogó el Reglamento (UE) 524/2013 y se modificaron los Reglamentos (UE) 2394/2017 y (UE) 1724/2018 para la supresión definitiva del ecosistema digital de Resolución de Litigios en Línea (RLL).

En consecuencia, el presente artículo de investigación pretende responder la siguiente pregunta: ¿cuáles son las principales razones para que la plataforma digital de Resolución de Litigios en Línea (RLL) ofrecida por la Comisión Europea para la gestión de conflictos entre consumidores y comerciantes haya sido suprimida si disponía de funcionalidades enmarcadas dentro de los mecanismos alternativos de solución de conflictos para la garantía formalista de los derechos de los consumidores? Al respecto se formula una hipótesis según la cual se considera que la plataforma digital de Resolución de Litigios en Línea (RLL) no contó con plena materialización iusteórica respecto de los derechos de los consumidores, dado que se trató de un riguroso diseño formalista basado en la Directiva 2013/11/UE que desconoce las dinámicas que formula la cotidianidad de las relaciones de consumo.

Para validar esta hipótesis se acoge como objetivo general de este artículo el siguiente: determinar las principales razones para que la plataforma digital de Resolución de Litigios en Línea (RLL) ofrecida por la Comisión Europea para la gestión de conflictos entre consumidores y comerciantes haya sido suprimida si disponía de funcionalidades enmarcadas dentro de los mecanismos alternativos de solución de conflictos para la garantía formalista de los derechos de los consumidores. Para desarrollar este objetivo general se adoptan los siguientes objetivos específicos de investigación a manera de estructura argumentativa del presente artículo: primero, delimitar desde el

payment services. The digital archives as means of protection for the cunsomer customer and citizens' (2022) 2021/2 EJPLT, 96-109.

[9] Algunas críticas que pueden ser identificadas se encuentran a continuación, sin pretender ser una lista taxativa: E Calderón, 'Resolución De Disputas En línea (ODR): Estándares éticos En El Ciberespacio' (2023) 46 REEI, 527-545. Además, pueden ser considerados los siguientes debates desde una perspectiva aplicada: L. Izzo, 'La tutela dell'utente degli strumenti di pagamento contro le transazioni fraudolente: problematiche giuridico-applicative e possibili evoluzioni' (2021) 1 2021/2 EJPLT, 10-32.

[10] En torno al análisis crítico de este tipo de plataformas para la gestión de conflictos se recomienda consultar a manera de referente el siguiente artículo de investigación: G Ortega, 'Análisis crítico de la plataforma europea de resolución de conflictos en línea' (2019) 29 IDP, 1-15.

[11] El siguiente trabajo de investigación puede ser tomado como referente de las críticas que sobre las plataformas de resolución de conflictos constituyen el estado del arte de este artículo, a saber: C Marqués 'La plataforma europea de resolución de litigios en línea (ODR): Su funcionamiento y retos de futuro' (2017) 3 Revista Iberoamericana de Derecho Informático, 75-96.

formalismo las funcionalidades que tuvo la plataforma digital de Resolución de Litigios en Línea (RLL) para promover la gestión del conflicto a través de mecanismos alternativos de solución de conflictos; y, segundo, analizar críticamente desde el antiformalismo las funcionalidades de la plataforma digital de Resolución de Litigios en Línea (RLL) enmarcadas en las disposiciones europeas vigentes actualmente para la protección de los derechos del consumidor. El desarrollo de estos objetivos se hará con un enfoque de investigación hermenéutico crítico, fundamentado en métodos cualitativos y con la revisión documental como principal estrategia de recolección de información.

2. Funcionalidades de la plataforma digital RLL de la Comisión Europea desde el formalismo.

La plataforma digital de Resolución de Litigios en Línea (en adelante RLL) de la Comisión Europea se originó en respuesta a la imperiosa necesidad de facilitar la efectividad de los derechos de los consumidores y comerciantes, en consonancia con las normas jurídicas europeas sobre resolución de litigios transfronterizos en materia de consumo y que se consolidan a partir de la Directiva 2013/11/UE [12] . Aunque parte de la comunidad jurídica puede considerar que es una herramienta para solucionar conflictos, en realidad estuvo llamada a cumplir un rol de mediación para que entre particulares se pudiese llegar a acuerdos. Esto se justifica al considerar que no se trató de una autoridad en sí misma, sino de un desarrollo tecnológico encaminado a apoyar a diferentes sujetos, en particular consumidores, para la gestión de sus conflictos en el marco de las normas jurídicas aplicables a cada caso[13]. En este sentido, RLL se consolidó como un ecosistema digital, definido como un espacio tecnológico con múltiples funcionalidades que han de ser gestionadas de manera directa por parte de los usuarios.

Si bien RLL respondió a un entramado complejo de normas sobre derecho del consumo consolidadas en la realidad europea según lo dispuesto por la Directiva 2013/11/UE, su surgimiento normativo directo se relaciona con el Reglamento 524 de 2013 de la Unión Europea y que exhorta a consolidar medios digitales para la gestión de conflictos de consumo en el espacio europeo en general[14]. Así, desde que inició el desarrollo tecnológico de RLL y entró en funcionamiento en 2016 bajo el marco de los Reglamentos de la Unión Europea referentes a relaciones de consumo en general. Entre otras características, RLL buscó mitigar el formalismo excesivo mediante un proceso

[12] Como complementado a las referencias antes incluidas y que contextualizan el RLL de la Comisión Europea, esta investigación hace un análisis crítico de los alcances de estos mecanismos extrajudiciales: W Nava, 'Los mecanismos extrajudiciales de resolución de conflictos en línea: su problemática en el derecho internacional privado' (2020) 13 ACDI, 1-34.

[13] Es posible profundizar en la experiencia europea desde la concepción alemana del asunto sistematizada en este artículo científico: M Stöber, 'La resolución alternativa de litigios en el derecho alemán y europeo' (2023) 15 Rev. Jurid. Mario Alario D'Filippo, 5-28.

[14] Los avances en investigación sobre la solución alternativa de conflictos a través de medios tecnológicos puede comprenderse en este artículo resultado de investigación: F Martín, 'Justicia digital post-covid19: El desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial' (2020) 2 REJUCRIM, 41-74.

accesible, fomentando así el antiformalismo en la resolución de disputas, proporcionando, al menos teóricamente, un entorno neutro y seguro para la comunicación y negociación entre las partes involucradas[15]. Por lo mismo, se esperó que su creación fortaleciera la confianza de los consumidores en el mercado único digital europeo, promoviendo una mayor expansión del comercio electrónico transfronterizo dentro de la Unión Europea.

Consecuentemente, es posible delimitar desde tres alcances las funcionalidades que tuvo RLL en relación con las apuestas jurídicas antes formuladas, a saber: primero, generar orientaciones teóricas a los usuarios en torno al derecho del consumo; segundo, permitir que las partes en conflicto pudiesen tender puentes de comunicación directo entre ellos; y, tercero, orientar acerca de posibles rutas de atención para los intereses y necesidades de los usuarios en caso en que el contacto directo no funcionara. En cuanto a la primera funcionalidad, RLL proporcionaba orientaciones teóricas detalladas a los usuarios sobre el derecho del consumo. Así, RLL ofrecía acceso a documentos legales, directrices y jurisprudencia relevante, lo cual esperaba permitir a los consumidores y comerciantes comprender mejor sus derechos y obligaciones en caso de disputas[16]. Además, la plataforma facilitaba herramientas interactivas y explicaciones prácticas que pretendían ayudar a los usuarios a comprender la gestión de conflictos de manera informada y autónoma. Esta función no solo fortalecía la educación legal de los usuarios, sino que también perseguía promover la transparencia y la equidad en las transacciones comerciales digitales, asegurando que todas las partes involucradas estuviesen debidamente informadas y protegidas bajo la legislación europea vigente.

Ahora bien, desde su segunda funcionalidad, RLL permitía que cualquier consumidor contara con un canal directo de comunicación con la contraparte con la cual tiene una disputa. En este sentido, RLL dispuso de funcionalidades avanzadas como mensajería electrónica y salas virtuales de negociación, diseñadas para facilitar un intercambio de información estructurado y confidencial[17]. Este enfoque no solo respaldaba la resolución expedita de conflictos transfronterizos, sino que también fomentaba, en teoría, la autonomía y participación directa de las partes involucradas en la búsqueda de soluciones enmarcadas en mecanismos alternativos de solución de conflictos autocompositivos[18]. De manera específica, RLL disponía de la posibilidad de acudir a la transacción, en calidad de arreglo directo, y a la mediación, en la cual las partes hacen acuerdos mientras que un tercero les habilita estrategias de

[15] Al respecto de estos avances en tecnología para la gestión de los conflictos en el contexto europeo se recomienda consultar: G Ortega, 'Análisis crítico de la plataforma europea de resolución de conflictos en línea' (2019) 29 *IDP. Revista De Internet, Derecho Y Política*, 1-15.

[16] Sobre la primera funcionalidad en torno a la información del derecho del consumo se han realizado algunas investigaciones recientes, entre las cuales se encuentra esta: S Peters, 'La evolución de la resolución alternativa de conflictos y la resolución de conflictos en línea en la Unión Europea' (2021) 12 *rev.ces derecho*, 3-17.

[17] Al respecto se pueden consultar productos de nuevo conocimiento como este: M Velicogna, 'Cross-border dispute resolution in Europe: Looking for a new "normal"' (2022) 12 *Oñati Socio-Legal Series*, 556-581.

[18] Para conceptualizar el sentido de los mecanismos alternativos de solución de conflictos con carácter auto compositivo se recomienda consultar: B Silva, 'Mecanismos alternativos de solución de conflictos. Análisis bibliométrico 2009-2018: base de datos Scopus' (2020) 10 *RIDE. Rev. Iberoam. Investig. Desarro.*, 1-23.

comunicación efectiva [19]. En consecuencia, RLL se planteó desde una perspectiva formal como una posibilidad de exaltar la voluntad de las partes contratantes para que gestionaran sus conflictos.

Esta concepción en torno a la autonomía de la voluntad que conllevaba RLL se adscribía a la naturaleza misma del derecho privado, según el cual las partes de una relación negocial son aquellas llamadas a determinar las consecuencias principales de sus compromisos contractuales [20]. Así, los contratos son realizados en el marco regulador de la ley, pero ella no llega a determinar todas las condiciones concretas en las que las partes acuerdan y solo tiene un carácter hermenéutico regulador desde requisitos generales que han de ser interpretados desde cada realidad[21]. En consecuencia, y considerando que los acuerdos que se realizan en el marco de un contrato son ley para las partes, los sujetos en disputa debían ser aquellos que de la misma manera en que contrataron tuviesen la posibilidad de hacer acuerdos adicionales para la gestión de sus conflictos[22]. No es un asunto menor que el derecho privado aplicable a estos casos determine que los contratos se deshacen como se hacen, guardando alineación en las posibilidades de creación, cumplimiento y disolución que las partes dentro del marco mínimo de la ley puedan realizar.

En consecuencia, cuando un usuario acudía a RLL para que lo pusiera en contacto con el otro sujeto contractual, el ecosistema digital no gestionaba su conflicto, sino que habilitaba los canales para que en el marco de la autocomposición las partes tuviesen la posibilidad de acordar una solución o, en caso de no tenerla, determinar entre ellos mismos una autoridad que resolviera su disputa[23]. En este punto, RLL confiaba en la voluntad de las partes y a ella añadía la buena fe que se esperaría de los sujetos que interactúan en el mercado, por lo cual les daba un tiempo perentorio de treinta (30) días para que este trámite fuera posible. Desde la perspectiva formalista que se ha venido mencionando, este número de días pretendía hacer énfasis en la necesidad de resolver los conflictos de manera pronta, para que el mercado pueda responder a dinámicas sanas de interacción y las personas alcanzaran posibilidades de justicia enmarcadas en la equidad lo más pronto posible[24]. Por lo tanto, RLL estaba diseñado desde la confianza en las partes, lo cual no solo tiene un efecto

[19] Sobre las funcionalidades para la gestión de la segunda funcionalidad sugerida para RLL se sugiere consultar este producto de nuevo conocimiento: J Camacho, 'Seguridad de la información en sistemas de resolución de disputas en línea (ODR): Revisión de la literatura y análisis a la luz del contexto colombiano' (2020) 41 *RIDE. Rev. Espacios*, 140-154.

[20] Al respecto de las fuentes del derecho comercial se recomienda consultar: J Perilla, 'Alineación iusteórica de las fuentes del derecho comercial' (2015) 53 Rev. *Derecho priv.,* 1-23.

[21] Los postulados del derecho privado en el cual se fundamentó esta afirmación del artículo se encuentran sistematizados a continuación: D Celis, 'La naturaleza de las reglas para la interpretación de los contratos: análisis sobre su alcance conceptual en la atribución de significado a cláusulas contractuales' (2022) 44 *derpri*, 117-141.

[22] Al respecto se sugiere consultar el capítulo referente a las fuentes de los derechos reales, en el cual se explica desde la teoría alemana la prevalencia de la voluntad de las partes sobre la ley en casos de negocios jurídicos: JSA Perilla-Granados, *Derecho de Sucesiones* (2nd edn, Universidad Sergio Arboleda 2017) 36.

[23] Para profundizar sobre el tema se sugiere consultar esta investigación disponible en línea y cuyos datos de identificación son los siguientes: J Conde, 'La plataforma europea de resolución de litigios en línea ¿alternativa efectiva para los consumidores?' (2020) 50 *Revista general de derecho procesal*, 1-18.

[24] Los debates en torno a los alcances de los mecanismos alternativos de solución de conflictos pueden ser analizados aquí: A Cerillo, 'Information Conflicts. Is Mediation a Solution? Lessons from the Catalan Experience' (2020) 24 *Deradm*, 293-312.

simbólico, sino que respondía a los principios más fundamentales del derecho privado.

Por lo anterior, se esperaba que RLL fuese el ecosistema digital para que las partes gestionaran y pusieran fin a sus conflictos a través de la materialización de las disposiciones jurídicas del derecho del consumidor. Solo, excepcionalmente, se consideraba que los treinta (30) días previstos para la autocomposición eran insuficientes, momento en el cual RLL de manera automática archivaba el caso. Y es en estos casos de archivo en el cual se activaba la tercera funcionalidad de RLL, dado que era fundamental orientar a las partes sobre cuál debía ser la ruta a tomar cuando el arreglo directo con mediación externa no daba por terminado el conflicto de consumo[25]. Así, se generaba una notificación automática en la cual se redireccionaba a cada uno de los usuarios, tanto el solicitante como su contraparte, para que pudieran decidir en torno a otras opciones posibles en las que no se descartaba que pudiesen llegar a un acuerdo directo o que activaran otras rutas con relevancia jurídica para la solución hetero compositiva de las problemáticas.

Entre las múltiples herramientas que se enunciaban por RLL para una solución posterior se encuentran los siguientes: Centros Europeos del Consumidor, para promover asesorías que llegan a contar con asistencia en disputas transfronterizas; Organismos de Resolución de Litigios, como una forma hetero compositiva que un tercero neutral llegue a decidir a través de medios tecnológicos acerca del problema; Red para la Resolución de Litigios Financieros, desde el contexto especializado de los bancos, aseguradoras e inversiones en bolsa; Organizaciones Nacionales de Consumidores, como fuentes adicionales de información y soporte para ejercer los derechos contemplados en las normas europeas; acciones judiciales, que conllevan onerosidad por parte del reclamante desde vías jurisdiccionales oficiales según el contexto en el cual se lleve a cabo el litigio; y la posibilidad de encontrar un abogado titulado en la Unión Europea, para celebrar con él un contrato de mandato para que sea quien, desde el ejercicio profesional del derecho, asuma la gestión definitiva de la situación.

Resulta especialmente relevante esta tercera funcionalidad, pues mantenía un mensaje de confianza hacia el usuario y determinaba que la inoperancia de la segunda funcionalidad no correspondía al final de las posibilidades de protección. En este sentido, se fortalecía la eficacia simbólica del contenido de RLL y su alcance formalista desde la teoría del derecho[26]. Esto se justificó en la medida en que se daba a entender al consumidor que en efecto las normas jurídicas existentes contaban con la posibilidad de responder a las problemáticas presentes en la realidad, generando un mensaje de completitud que bien podía adscribirse al positivismo como escuela propia del derecho

[25] Sobre las diversas rutas de solución de conflictos en el caso de derecho del consumidor, es posible analizar esta investigación aplicada: G Izquierdo, 'Los derechos del consumidor en los procesos de evaluación de solvencia mediante el tratamiento automatizado de datos contenidos en la Directiva (UE) 2023/2225' (2024) 49 *Revista CESCO*, 80-106.

[26] Es posible profundizar en los debates en torno al formalismo en esta investigación: JSA Perilla-Granados, 'El Estado retado desde el constructivismo antiformalista: legitimidad y convicción' (2021) 14 *Criterios*, 21-36.

privado[27]. Esta pretendida completitud se tiende a asegurar desde la existencia de normas jurídicas creadas por el legislador tradicional, el cual está dotado de legitimidad suficiente para impactar la realidad y promover relaciones de consumo con garantía de derechos. Y, en consecuencia, se esperaría de parte del usuario de RLL una interpretación mimética de las normas jurídicas, confiando que desde su contenido se resolverán los conflictos.

En este orden de ideas, es posible considerar que RLL estuvo contemplada desde un alcance formalista para la garantía de los derechos de los sujetos involucrados en relaciones de consumo y manteniendo eficacias simbólicas en torno a los alcances que las normas jurídicas tienen para la gestión de los conflictos. Parecería ser que los desarrollos de tres funcionalidades tenían la posibilidad de garantizar los derechos de los consumidores, manteniendo posibilidades para que la realidad del mercado respondiera a la autonomía de la voluntad y a la buena fe contractual. Por lo tanto, tanto los Estados como el conglomerado social podían tener confianza en el aporte que RLL daba a sus relaciones en el mercado. Sin embargo, estas bondades de RLL formuladas desde el formalismo como iusteoría del derecho encontraron posibilidades de análisis crítico desde el alcance propio del antiformalismo, que llevaron a la desfinanciación de este ecosistema digital.

3. Análisis antiformalista de las funcionalidades de RLL desde los derechos del consumidor.

Según se evidenció en la sección anterior, RLL se consolidó como un ecosistema digital cuyos usuarios son cualquiera de los sujetos de las relaciones de consumo; podían acudir a esta herramienta tecnológica tanto los consumidores como los comerciantes para gestionar los conflictos que se tenían entre ellos. Sin embargo, debe tenerse en cuenta que los usuarios principales de RLL eran los consumidores, buscando la materialización de los derechos que consideraban les fueron vulnerados o estaban en riesgo de vulneración. En este sentido, esta plataforma será analizada desde cada una de sus funcionalidades desde un enfoque antiformalista y que tiene en cuenta los derechos de los consumidores a los cuales pretendía responder la Comisión Europea con la implementación de RLL. Para estos efectos, a continuación se delimitará el alcance antiformalista que se opone al formalismo referenciado en la primera sección, para que a partir de allí sea posible analizar puntualmente cada una de las funcionalidades desde una perspectiva crítica enmarcada en las normas de protección al consumidor como usuario principal de RLL.

Siendo coherentes con el alcance metodológico formulado para esta investigación, debe considerarse en un primer lugar que la teoría jurídica aplicable a áreas como el derecho privado se enfrenta actualmente a una

[27] Sobre la teoría de la comunicación política con eficacia simbólica de las normas jurídicas se recomienda consultar: D Páramo, 'El consumo como entidad simbólica' (2021) 50 *Pensam. Gest.*, 1-3.

dicotomía entre el formalismo y el antiformalismo[28]. Se trata de dos iusteorías que se componen de elementos de diferentes escuelas del derecho, consolidando un entramado completo de criterios hermenéuticos para analizar el alcance de determinada norma jurídica. Según se vio antes, el formalismo encuentra su fundamentación en las escuelas del positivismo y del naturalismo que llevan a la mímesis interpretativa[29]. En consecuencia, el derecho es entendido con una aspiración de perfección, que se legitima por un legislador tradicional que lleva a que los operadores jurídicos pretendan encontrar soluciones a sus conflictos desde lo dispuesto por la norma escrita. Y, tal como se evidenció antes, este era el alcance que podía ser identificado desde el diseño con el que cuentó RLL según las tres funcionalidades planteadas.

Ahora bien, en contraposición al formalismo, el antiformalismo se compone de elementos desarrollados por escuelas como las siguientes: el realismo, que comprende que las normas jurídicas no son un entramado de disposiciones objetivas, puesto que están mediadas por influencias políticas, económicas, sociales, entre otras[30]; el utilitarismo, el cual se centra en maximizar los efectos de una ley en el bienestar general desde parámetros que exigen la minimización de efectos negativos en el conglomerado social[31]; y el funcionalismo, el cual pretende determinar si las normas jurídicas en efecto responden a los intereses y necesidades para las cuales fueron formuladas[32]. Cada una de estas escuelas, sin tratarse de un asunto lineal, aporta a que desde el formalismo se otorgue una naturaleza abierta al derecho, es decir, reconoce que no puede resolver todos los casos debido a la existencia de lagunas. En consecuencia, para solucionar un caso se debe acudir a múltiples fuentes jurídicas de manera auténtica, sin limitarse a aquellas creadas por el legislador desde una perspectiva tradicional.

Por esto mismo es que desde la iusteoría antiformalista resulta reprochable, o por lo menos sospechoso, que RLL se planteara como una estrategia holística para la materialización de los derechos de los consumidores[33]. Así, resulta fundamental analizar críticamente cada una de sus funcionalidades más allá de la concepción mimética que justificó desde una perspectiva tanto teleológica como gramatical las bondades pretendidas para RLL. Así, y haciendo referencia a la primera funcionalidad referente a la información suministrada por el aplicativo, debe analizarse en un primer momento que si bien los comerciantes

[28] La comprensión entre las pugnas existentes entre el formalismo y el antiformalismo pueden ser analizadas en esta investigación aplicada: J Perilla, 'Los centennials como un reto antiformalista para las facultades de derecho' (2021) 8 *Rev. Pedagog. Univ. Didact. derecho.*, 11-28.

[29] La conceptualización de la iusteoría del formalismo puede ser profundizada aquí: J Etcheverry, 'Formalismo, activismo y discrecionalidad judicial' (2020) 29 *Díkaion.*, 336-351.

[30] Como una manera de conceptualizar la escuela jurídica del realismo se sugiere consultar: A Caballero, 'Nuevo realismo jurídico: una teoría jurídica prometedora para la investigación interdisciplinar y empírica sobre el derecho en la práctica' (2022) 16 *Novum Jus.*, 209-228.

[31] El utilitarismo ha tenido diferentes vertientes doctrinales, pero para efectos de esta investigación se recomienda profundizar en este alcance más tradicional: F Murillo, 'El Utilitarismo Clásico de Jeremy Bentham: Una discusión y revisión historiográfica alrededor del utilitarismo, su oposición a la filosofía de los derechos naturales y su postura frente a la redistribución de la riqueza' (2022) 55 *Prax. filos.*, 169-188.

[32] La escuela funcionalista que se acoge en esta investigación es delimitada a continuación: H Cadenas, 'La función del funcionalismo: una exploración conceptual' (2016) 18 *Sociologías*, 196-214.

[33] Las críticas antiformalistas son esperables de manera transversal al análisis del derecho, para lo cual se sugiere consultar el siguiente artículo: J Perilla, 'La enseñanza del derecho procesal penal desde el constructivismo antiformalista' (2024) 10 *Revista Brasileira de Direito Processual Penal*, 1-32.

pueden ser considerados como expertos en este tipo de normas, los consumidores se alejan de esa experticia y se consolidan como consumidores medios que se centran en hacer una lectura confiada de la letra grande[34]. En este sentido, presentar información técnica a un consumidor medio no necesariamente aseguraba que pueda tener una comprensión total del mensaje que pretendía ser transmitido desde RLL.

En este mismo sentido se debe considerar que los consumidores medios han de ser clasificados por edades y contextos en los cuales se encuentren, por ejemplo, realidades urbanas o rurales[35]. Esto se justifica en que la categoría de consumidor es una de las más diversas, por incluir en sí misma a todos los sujetos que no solo hacen parte de la unión europea, sino también extranjeros no europeos que puedan ejecutar relaciones de consumo en estos casos[36]. Y aquí es donde se refuerza el cuestionamiento a la manera en que estaba diseñado RLL, pues desde una idea de diseño universal no atiende a las características puntuales que pueden tener los diferentes tipos de consumidores. Aunque el lenguaje utilizado por RLL podía ser comprensible para determinados consumidores, pensado por los diseñadores del ecosistema, se requeriría contemplar que otros consumidores responden a segmentaciones que puedan hacer ajustes razonables al manejo de la información. Se trata de una exigencia que se realiza en el mercado a los mismos comerciantes, por lo cual se esperaría que también se viera materializada a plenitud en el contenido de RLL.

A estos cuestionamientos sobre el alcance de la información de la primera funcionalidad, se pueden adicionar otros referentes a la segunda funcionalidad encaminada a propiciar contactos entre consumidores y comerciantes en conflicto. El principal cuestionamiento es que esta funcionalidad tenía una confianza notablemente alta en los principios que rigen el derecho privado, pero no contemplaba las condiciones concretas del ejercicio de las relaciones contractuales y sus dinámicas de poder[37]. Aunque se esperaba obtener respuesta de aquella parte contractual contactada a través de RLL, lo cierto es que esto no se veía materializado en las prácticas generalizadas de las relaciones de consumo. De manera particular, la mayoría de los casos que eran presentados bajo la segunda funcionalidad en RLL fueron archivados, entre otras razones, porque la parte que era requerida no estaba obligada a responder; en realidad, ni siquiera estaba obligada jurídicamente a revisar el mensaje que es remitido.

En consecuencia, las obligaciones de esta segunda funcionalidad quedaban dentro del campo de lo natural o moral, sin tener realmente estrategias de coerción para que la autocomposición pudiese ser una realidad. Esto es especialmente relevante en la medida en que no se encontraba mayor

[34] Para comprender el alcance del consumidor medio se recomienda revisar este artículo de investigación científica: J Perilla, 'Construcción antiformalista del consumidor medio' (2015) 54 Rev. *Derecho priv.,* 1-23.
[35] Como un desarrollo de los alcances de consumidor medio por grupos poblacionales se recomienda consultar: D Báez, 'El menor de edad en la relación de consumo: una revisión a la clasificación de consumidor vulnerable' (2023) 25 *Estud. Socio-Juríd.,* 1-19.
[36] La conceptualización diversa del consumidor puede ser comprendida en este resultado de investigación: M Otero, 'Big Data: atrapando al consumidor' (2020) 27 *Turismo y sociedad.,* 183-186.
[37] Las relaciones de poder generan subordinaciones en las relaciones de consumo y un ejemplo de ellas se encuentra a continuación: E Quintero, 'Relación entre percepción de poder y prácticas de consumo en la categoría de diversión de personas LGBT' (2016) 23 *Suma Psicol.,* 90-100.

diferencia al contactar a la contraparte de manera directa o a través de RLL, por lo cual se podían estar generando expectativas infundadas en torno a la funcionalidad del ecosistema digital objeto de análisis. Y a esto se adiciona que si la mayoría de los usuarios de RLL eran consumidores, es decir, la parte débil de la relación contractual, la Comisión Europea no estaba generando ninguna estrategia que se pudiese considerar efectiva para superar la subordinación a la cual está sometido este sujeto respecto del comerciante que supuestamente está inaplicando el derecho del consumidor. Por lo tanto, la segunda funcionalidad no aseguraba realmente que haya una solución oportuna y de fondo a la situación, pues estaban relacionándose dos sujetos que carecen de una igualdad negocial para superar sus disputas.

Al considerar estos cuestionamientos en torno a las dos primeras funcionalidades de RLL, se tenía como un efecto esperable que la mayoría de los consumidores que acuden a este ecosistema tuvieran que hacer uso de la tercera funcionalidad y que se refería a recibir orientación sobre rutas adicionales para la gestión del conflicto. En este escenario en particular se debe considerar primero que RLL sugería llevar a cabo ciclos que no aseguraban una solución de fondo, dado que insistían desde su diseño instruccional en la necesidad de intentar cuantas veces sea necesario el arreglo directo y, según se planteó antes, no era una estrategia que desde la exigibilidad jurídica pudiese otorgar soluciones. Y a esto se suma que una vez agotada la segunda funcionalidad de RLL, se sugería acudir a otras estrategias que bien podrían haberse intentado antes y sin necesidad de esperar treinta (30) días para alcanzar un acuerdo que difícilmente se podía materializar. En realidad, el arreglo directo propio de la segunda funcionalidad de RLL no era un requisito de procedibilidad para ejercer otras rutas propias de la tercera funcionalidad y sugeridas una vez que se archivaba el caso.

Sobre el particular resulta especialmente reprochable que cuando RLL notificaba del archivo del caso al solicitante, le indicaba que podía consultar otras formas de resolver el conflicto y en esas otras formas volvía a referirse nuevamente a la segunda funcionalidad de RLL que ya resultó fallida. Por lo tanto, pareciera ser que RLL estaba formulado desde una perspectiva genérica y no atendiendo a todas las variables que podían existir en las relaciones de consumo que son marcadas por la diversidad de los involucrados. En este sentido, una persona que haya agotado las dos primeras funcionalidades de RLL y que no haya solucionado su caso, no habrá tenido ningún tipo de avance, lo cual se ve agravado en la medida en que la tercera funcionalidad parecía sugerir un ciclo que no otorgaba herramientas suficientes para que los usuarios pudiesen solucionar efectivamente sus conflictos. De ahí que resultó importante determinar si en tales condiciones, RLL tenía un impacto real que pudiera materializar los derechos de los consumidores y no solo legitimar la subordinación que los comerciantes tienen frente a ellos.

Se trata de un debate que desde el antiformalismo llevó a transformaciones concretas para la gestión de casos por parte de RLL, pues de nada servía tener un conjunto robusto de normas que reconocen derechos del consumidor si los ecosistemas digitales previstos para gestionar conflictos tenían utilidades casi nulas desde la práctica. En últimas, si un ecosistema digital como RLL no estaba aportando soluciones de fondo marcadas por la efectividad a situaciones que

terminarían siendo gestionadas por medios tradicionales, debía evaluarse la pertinencia de mantenerlo o hacer los ajustes en el sentido antes planteado. Para ello no fue suficiente hacer una reforma normativa desde un alcance formalista, pues resultó fundamental generar validaciones prácticas desde y para las realidades de las relaciones de consumo que se pretendían impactar. Hasta tanto no se aseguren impactos decididos sobre las expectativas generadas desde la formalidad del derecho del consumo, será muy complejo aportar a que las normas jurídicas sean materializadas más allá de la literalidad del texto escrito. Resulta fundamental generar estrategias para consolidar otras herramientas digitales que en reemplazo de RLL aseguren una plena materialización de los derechos de los consumidores desde el antiformalismo.

4. Conclusiones.

El derecho del consumo ha sido identificado como relevante en el contexto de la Comunidad Europea, razón por la cual se han generado conjuntos de normas jurídicas que abordan diferentes alcances de las relaciones existentes en el mercado. Esto ha llevado a concluir que las normas trasnacionales aplicables a estas situaciones son robustas, dado que reconocen derechos y establecen obligaciones para los intervinientes en la contratación que incluye por lo menos un consumidor. Y en el marco de estas normas jurídicas con alcance proteccionista, como es de esperarse, se presentan conflictos que requieren gestiones efectivas para asegurar que las pretensiones de las autoridades legislativas europeas se cumplan. Por esta razón, en 2013 se estableció la necesidad de consolidar desarrollos tecnológicos tendientes a apoyar a los sujetos de las relaciones del consumo a gestionar sus disputas. Y desde esa fecha se desarrolló desde la Comisión Europea una plataforma digital de Resolución de Litigios en Línea (RLL), la cual entró en funcionamiento en 2016, pero a la fecha se aprobó su desfinanciación.

RLL estuvo diseñada para cumplir tres funcionalidades principales, a saber: primero, otorgar información a los consumidores y comerciantes acerca del contenido de las normas jurídicas referentes al derecho del consumo aplicables al mercado de la Unión Europea; segundo, habilitar canales de comunicación directos para que en caso de una disputa los consumidores pudiesen solucionar de manera autocompositiva con los comerciantes sus conflictos de manera pronta y en el marco de las normas jurídicas aplicables; y tercero, sugerir rutas adicionales para que los sujetos que no podían solucionar sus problemas a través de las dos funcionalidades anteriores tuvieran la posibilidad de alcanzar una solución de fondo. Se trató, desde una perspectiva formal, de un alcance holístico para la gestión del conflicto, razón por la cual RLL era considerado no solo una plataforma, sino un ecosistema digital en sí mismo. Los ecosistemas digitales están diseñados para generar interacciones múltiples en torno a asuntos propios de la realidad en la cual están inmersos.

Y desde una perspectiva formalista, estas tres funcionalidades cumplían a cabalidad los lineamientos jurídicos establecidos por las autoridades europeas para el fortalecimiento de las relaciones de mercado. Esto se justifica al considerar que la iusteoría del formalismo se fundamenta en las escuelas del

positivismo y del naturalismo, llevando a considerar que el derecho es un entramado de normas con aspiración de perfección con la vocación de solucionar de fondo las disputas que se puedan presentar entre consumidores y comerciantes. Esto se justifica en la medida en que las normas jurídicas son creadas por un legislador tradicional, el cual contempla garantismos expresos para que desde interpretaciones miméticas se tenga eficacia simbólica de lo preceptuado. Por lo tanto, RLL tenía la función se asegurar que estas características se cumplieran de cara a un conglomerado social que esperaba tener allí una posibilidad de gestión de conflictos suficiente.

Sin embargo, desde la iusteoría del antiformalismo, fundamentada en escuelas como el realismo, el utilitarismo y el funcionalismo, se reconocieron límites más allá del diseño abstracto de RLL. De manera particular se formularon cuestiones críticas en torno a la falta de segmentación de los destinatarios de la información, reduciendo la posibilidad de un impacto suficiente de la primera funcionalidad y para la diversidad de consumidores que pueden acceder a RLL. Además, en cuanto a la segunda funcionalidad, se determinó que el arreglo directo se circunscribía a un asunto de obligaciones naturales o morales, por lo que carecían de auténticos alcances que asegurasen que ambas partes en pugna pudieran negociar desde posiciones equitativas. Y, finalmente, la tercera funcionalidad sugería la configuración de ciclos tendientes a acudir a arreglos directos que no funcionaron y llevaron a deslegitimar en sí mismo el sentido que RLL podía tener dentro de las aspiraciones para las que fue creado. En realidad, con las falencias identificadas no era claro que fuese necesario acudir a este ecosistema digital, pues bien pudo prescindirse de él para procurar soluciones más oportunas por otros medios de alcance más tradicional como la actividad judicial.

Con fundamento en estas conclusiones es posible plantear que se respondió a cabalidad la pregunta de investigación y el objetivo general que orienta este artículo científico, por lo cual se acepta la hipótesis según la cual la plataforma digital de Resolución de Litigios en Línea (RLL) no contó con plena materialización iusteórica respecto de los derechos de los consumidores, dado que se trató de un riguroso diseño formalista basado en la Directiva 2013/11/UE que desconoce las dinámicas que formula la cotidianidad de las relaciones de consumo. En este sentido, se requieren acciones concretas que trasciendan la abstracción del diseño tecnológico de RLL para asegurar impactos concretos desde y para la realidad que pretende alcanzar. Si bien se reconoce que RLL fue un avance importante para la garantía del derecho del consumo, resulta fundamental generar fortalecimientos antiformalistas que aseguren el cumplimiento de los fines a los cuales se ha de responder desde una gestión del conflicto oportuna, efectiva y pronta esperable para contextos como el europeo.

LIST OF AUTHORS OF THIS EJPLT ISSUE

DAVIDE ACHILLE – Associate Professor of Private Law, Università del Piemonte Orientale, Italy.

MIGUEL ÁLVAREZ ORTEGA – Associate Professor, Kyoto University School of Law, Japan. Profesor Contratado Doctor, Universidad de Sevilla, Spain.

ALICE ANGELINI – Ph.D. student in Criminal Law, University of Insubria, Italy.

ILARIA AMELIA CAGGIANO – Full Professor of Private Law, Suor Orsola Benincasa University of Naples, Italy. Vice-Director, Research Centre in European Private Law (ReCEPL), Italy.

FERNANDO CARBAJO CASCÓN – Full Professor of Commercial Law, Universidad de Salamanca, Spain.

GIUSEPPE CORASANITI – Full Professor of Philosophy of Digital Law, Universitas Mercatorum, Italy. Full Professor of Artificial Intelligence and Law, LUISS Guido Carli, Italy.

BOŠTJAN DELAK – Assistant Professor, Faculty of Information Studies, Slovenia.

TOMMASO DE MARI CASARETO DAL VERME – Research Fellow in Private Law, University of Trento, Italy.

MATJAŽ DREV – Ph.D., Information Security Consultant, Center for Healthcare Informatics, National Institute of Public Health, Slovenia.

MANOLITA FRANCESCA – Full Professor of Private Law, Università degli Studi di Foggia, Italy.

MARIA CRISTINA GAETA – Appointed Lecturer in Green Law and Green Mobility, Module Leader Jean Monnet Chair EUGREENEXT, Università degli Studi Suor Orsola Benincasa. Senior Researcher, Research Centre in European Private Law (ReCEPL), Italy.

LUCILLA GATT – Full Professor of Private Law, Suor Orsola Benincasa University of Naples, Italy. Director, Research Centre in European Private Law (ReCEPL), Italy.

VAHID AKEFI GHAZIANI – Pre-doctoral candidate, Torino International University College of Turin (IUC), Italy. Attorney at law, Central Bar Association of Iran, Iran.

OLEKSII VOLODYMYROVYCH KOSTENKO – Associate Professor, National Aviation University, Ukraine.

CATERINA MURGO – Associate Professor of Private Law, Università degli Studi di Pisa, Italy.

ANNA CARLA NAZZARO – Full Professor of Private Law, Università degli Studi Internazionali di Roma, Italy.

LUCA NIVARRA – Full Professor of Private Law, University of Palermo, Italy.

JUAN SEBASTIÁN ALEJANDRO PERILLA GRANADOS – Associate Professor, Universidad Tecnológica de Bolívar, Colombia.

FRANCESCA PRATESI – Researcher, Institute of Information Science and Technologies "Alessandro Faedo" (ISTI), National Research Council, Italy.

ROBERTA SAVELLA – Research Fellow Project SoBigData++, Institute of Information Science and Technologies "Alessandro Faedo" (ISTI), National Research Council, Italy.

DALIBOR STANIMIROVIĆ – Associate Professor, Faculty of Public Administration, University of Ljubljana, Slovenia.

ROBERTO TRASARTI – First Researcher, Institute of Information Science and Technologies "Alessandro Faedo" (ISTI), National Research Council, Italy.

EMILIANO TROISI – Ph.D., Suor Orsola Benincasa University of Naples, Italy. Junior Researcher, Research Centre in European Private Law (ReCEPL), Italy.