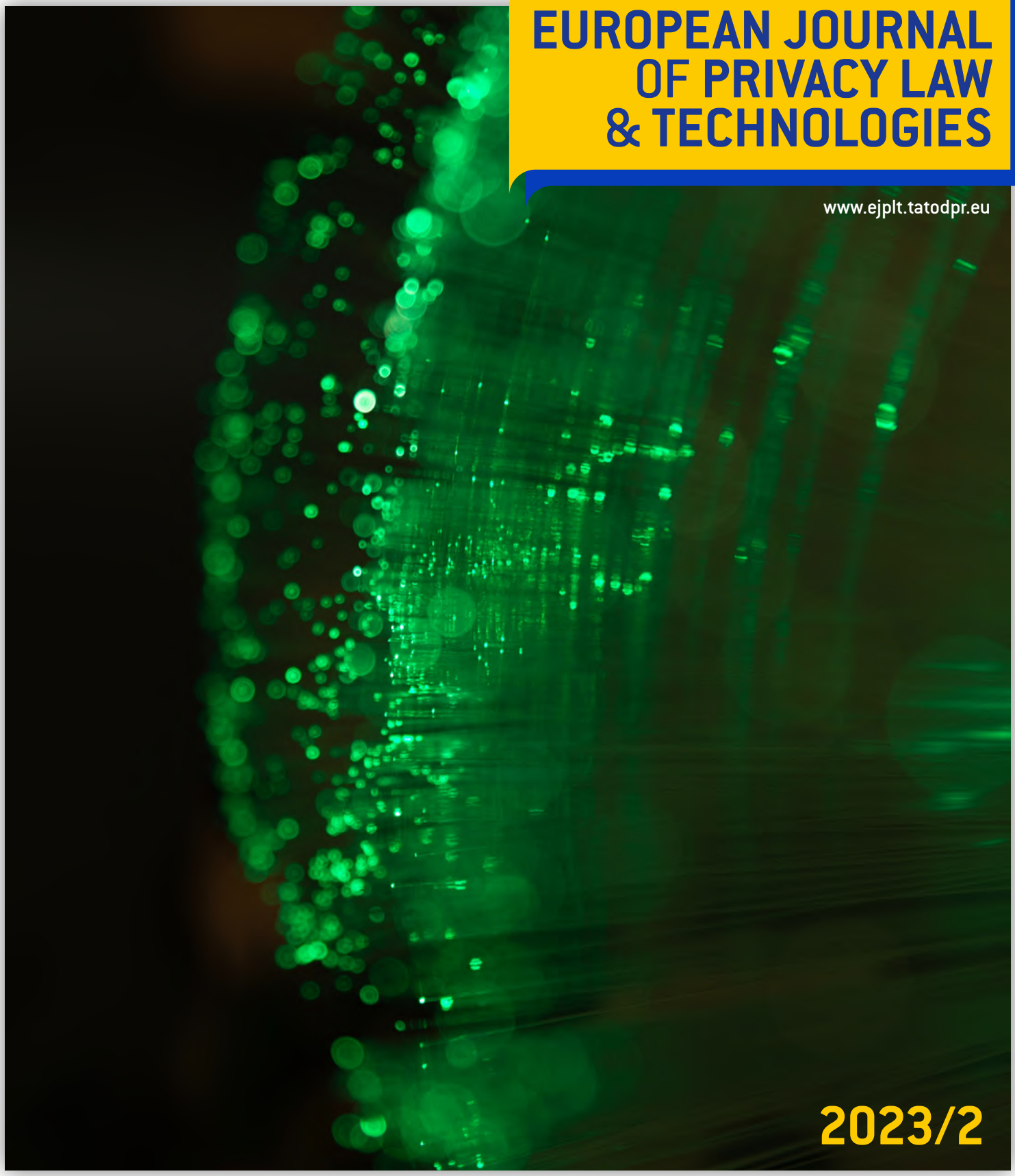
ISSN: 2704-8012

SUOR ORSOLA
BENINCASA
UNIVERSITÀ EDITRICE

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu



2023/2

EJPLT
ISSN: 2704-8012

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2023/2

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



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*

Editing Luciana Trama

Design Flavia Soprani

Development Maria Teresa Lo Conte

© Copyright 2023 by Suor Orsola Benincasa Università Editrice, published in December 2023
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*
Free access to the Issue at: *www.ejplt.tatodpr.eu*

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

ADVISOR BOARD – SCIENTIFIC COMMITTEE

Prof. Pasquale Arpaia – Università degli Studi di Napoli Federico II, Italy
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

REFEREES

Prof. Jeremy Antippas – Université de Bretagne Sud, France
Prof. Miguel Álvarez Ortega – Kyoto University, Japan, and Universidad de Sevilla, Spain
Prof. Carlos Antonio Agurto Gonzáles – Universidad Nacional Mayor de San Marcos, Peru
Prof. Andrea Bertolini – Scuola Superiore Sant'Anna di Pisa, Italy
Prof. Avv. Giuseppina Capaldo – Sapienza Università di Roma, Italy
Prof. Giovanna Capilli – Università San Raffaele di Roma, Italy
Prof. Cristina Caricato – Sapienza Università di Roma, Italy
Prof. Roberto Carleo – Università degli Studi di Napoli Parthenope, Italy
Prof. Georges Cavalier – Université de Lyon, France
Prof. María Dolores Cervilla Garzón – Universidad de Càrdiz, Spain
Prof. Maria Antonia Ciocia – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Giovanna D'Alfonso – Università degli Studi della Campania Luigi Vanvitelli, 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. Giovanni Iorio – Università degli Studi di Milano Bicocca, Italy
Prof. Arndt Künnecke – Hochschule des Bundes für öffentliche Verwaltung, Germany
Prof. Martin Maguire – University of Loughborough, United Kingdom
Prof. Giovanni Martini – Università degli Studi della Campania Luigi Vanvitelli, Italy
Prof. Paola Manes – Alma Mater Studiorum Uiversità di Bologna, 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

EJPLT
ISSN: 2704-8012

European Journal of Privacy Law & Technologies

Prof. Nora Ni Loideain – Institute of Advanced Legal Studies of London, United Kingdom
Prof. Taiwo Oriola – University of Derby, United Kingdom
Prof. Francesco Rossi – Università degli Studi di Napoli Federico II, Italy
Prof. Maria A. Scagliusi – Universidad de Sevilla, Spain
Prof. Sara Tommasi – Università del Salento, 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

COORDINATOR OF THE EDITORIAL BOARD

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

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. David T. Karamanukyan – Siberian University, Russian Federation
Prof. Maria Ioannidou – Queen Mary University of London, United Kingdom
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. 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. 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. 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. (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. (c) Emanuele Garzia – Università Suor Orsola Benincasa di Napoli, 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) Avv. Valeria Manzo – Università degli Studi della Campania Luigi Vanvitelli, 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) Emiliano Troisi – Università Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Chiara Vitagliano – Università degli Studi di Napoli l'Orientale, Italy

pp.

Section I: **Articles**

UGO PAGALLO, JACOPO CIANI SCIOLLA – *Anatomy of web data scraping: ethics, standards, and the troubles of the law. | Anatomia del web data scraping: etica, standard e problemi della legge.* 1

ROBERTO CARLEO – *The AGCOM regulation on "fair compensation": a co-regulation model in search of efficiency. | Il regolamento AGCOM sull'"equo compenso": un modello di co-regolazione in cerca di efficienza.* 20

ROBERTO CASO – *Diritto, politica ed economia dell'innovazione tecnologica: 1940, 1980, 2020. | Law, policy and economics of technological innovation: 1940, 1980, 2020.* 56

ROBERTO SENIGAGLIA – *Rischi identitari per la persona minore d'età nell'ambiente digitale. | Identity risks for the minor in the digital environment.* 62

EMILIO TOSI – *Dati personali e contratto: un ossimoro apparente. | Personal data and contract: an apparent oxymoron.* 71

ANDREA BORRONI, FABIO ZAMBARDINO – *Distributed Ledger Technologies (DLTs) and right to health: the impact of blockchain in the healthcare sector. | Distributed Ledger Technologies (DLTs) e diritto alla salute: l'impatto della blockchain nel settore sanitario.* 93

LUCILLA GATT, ILARIA AMELA CAGGIANO, MARIA CRISTINA GAETA, LIVIA AULINO, EMILIANO TROISI – *The possible relationships between law and ethics applied to AI. | Le possibili relazioni tra legge ed etica applicate all'IA.* 111

PAOLA GRIMALDI – *L'impatto delle criptovalute sull'ecosistema: analisi e possibili soluzioni. | The impact of cryptocurrencies on the ecosystem: analysis and possible solutions.* 121

FRANCO TRUBIANI – *Cloud Computing Services: towards a Digital Sustainability under EU Digital Law. | I servizi di cloud computing: verso la sostenibilità digitale nell'ambito della Strategia Digitale Europea.* 142

GIANLUCA MONTANARI VERGALLO, PASQUALE RICCI – *L'accertamento del nesso causale nei danni alla persona da inquinamento. | The assessment of causation between biological damage and pollution.* 156

LUCILA INÉS CÓRDOBA, ADRIANA SYLVINA MÓRON, IRENE COPPOLA – *Qualche considerazione critica sull'eredità digitale, tra patrimonio e dati un complicato bilanciamento di interessi nella tematica testamentaria. | Some critical considerations on digital inheritance, between assets and data a complicated balancing of interests in testamentary matters.* 169

Section II: **Focus papers**

ATTILIO ALTIERI – *Lo stato di automazione del processo civile e delle procedure concorsuali nell'interazione tra parti pubbliche e private. | The progress of automation of civil and insolvency proceedings in the interaction between public and private actors.* 187

ABIGAIL OWUSU – *Data sharing in the personal data economy. Does sharing mean caring? | La condivisione dei dati nell'economia dei dati personali. Condividere vuol dire prendersi cura?* 217

ANTONGIULIO LOMBARDI – *Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra GDPR e AI Act. | Data protection regulation and artificial intelligence regulation: relationships, similarities and differences between GDPR and AI.* 240

ANTONELLA DI CERBO – *La tutela dell'identità nell'ambiente digitale alla luce delle norme europee. | Identity protection in the digital environment in light of European Union regulation.* 253

List of authors 266

SECTION I
ARTICLES

Pagallo U, Ciani Sciolla J, 'Anatomy of web data scraping: ethics, standards, and the troubles of the law' (2023) 2 EJPLT, 1 - 19.
DOI: https://doi.org/10.57230/EJPLT232PS

EJPLT
ISSN 2704-8012



Anatomy of web data scraping: ethics, standards, and the troubles of the law

Anatomia del web data scraping: etica, standard e problemi della legge

UGO PAGALLO
Full Professor of Philosophy of Law, Law and Technology and Legal Theory
University of Turin
Member of the Nexa Center for Internet and Society Board of Trustees

JACOPO CIANI SCIOLLA
Researcher in Philosophy of Law and Legal Informatics
University of Turin
Adjunct Professor at ESCP
Turin Campus
Fellow of the Information Society Law Center
University of Milan

Abstract

The paper examines the ethical and legal issues raised by web scraping technology. Attention is drawn to some landmark rulings to emphasize that jurisdictions such as the US and the EU Member States tackle issues of scraping from different perspectives. Although most litigation involves IP law, in particular copyright and the rights of database producers, scraping can also raise problems of data protection, unfair competition, and public or criminal law. Besides, many of such issues may fall into the gaps of the legal system. Accordingly, the paper aims to provide an overall framework for the ethical and legal issues of scraping, to take sides between 'good' and 'bad' uses of technology and, on this basis, flesh out the legal hard cases of the field.

L'articolo esamina le questioni etiche e legali del data scraping attraverso l'analisi della giurisprudenza rilevante, per mostrare come gli USA e l'UE affrontino il fenomeno muovendo da prospettive molto diverse. Sebbene gran parte delle controversie riguardi la proprietà intellettuale, lo scraping solleva altresì questioni di protezione dei dati personali, concorrenza sleale e diritto penale. Il contributo evidenzia le lacune normative e le questioni etiche e legali da dirimere per distinguere tra usi "buoni" e "cattivi" della tecnologia, delineando al contempo i casi c.d. difficili.

© The author(s) 2023, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: data ownership; data scraping; web harvesting; data grabbing; intellectual property; data protection; trade secret; data access; data ethics; standards.

Summary: Introduction to data extraction via web scraping. – 1. The ethics of data scraping. – 2. The law of data scraping. – 2.1. Unfair competition of metasearch engines, or the Ryanair saga. – 2.2. Contractual liability: Are the website terms and conditions binding for the scraper? – 2.3. Non-contractual liability: Common law versus civil law approaches toward data scraping. – 2.4. Copyright over data and datasets. – 2.5 The database sui generis right. – 2.5.1. Substantiality of the investment. – 2.5.2 Substantiality of the extraction. – 2.6 The nature of scraped data: personal, public, or secret. – 2.6.1. The scraping of personal data. – 2.6.2. The scraping of data as an essential facility. – 2.6.3. The scraping of data kept secret. – 3. Discussion. – Conclusions.

Introduction to data extraction via web scraping.

*The notion of 'data scraping' can be understood as the extraction of data from a website to process, analyze, and present such data as useful information, especially for commercial purposes. Web services gather information from data hosts-websites that store or house target data, either by parsing or by scraping such data. Parsing generally refers to the collection of information through a series of formalized data requests and using application programming interfaces ('APIs'). Data structures, like Extensible Markup Language, or XML feeds, suited for automated computer processing, provide the format through which data can be efficiently stored, searched, and shared. However, such data interchange may not be available because of opposing interests of data holders or owners. Data scraping circumvents this problem by automatically extracting useful information from the Hyper Text Markup Language ('HTML') code that most websites display. This automated process, also called web crawling, harvesting, or data grabbing, is carried out by bots, web crawlers or web spiders.

Web scrapers typically take something out of a webpage to use it for another purpose, e.g., copying names and phone numbers, or companies and their URLs, to make a list, known as 'contact scraping'. Popular metasearch engines or search aggregators, such as Skyscanner and Booking.com, hinge on data scraping software to retrieve and aggregate search results of online travel agencies. Since these services depend on third parties' data, data holders often deem screen scraping illegitimate. As a result, a battle between website developers and scraping developers has followed, and still, from a legal viewpoint, the terms of this battle look uncertain.

* Ugo Pagallo wrote paras. 2 and 4; Jacopo Ciani Sciolla wrote paras. 3.1-3.6. All authors wrote paras. 1 and 5 and have read and agreed to the published version of the manuscript.

Correspondingly, the paper aims to deepen the normative issues[1], i.e., both moral and legal, brought about by data scraping, according to a twofold approach. On the one hand, the focus is on applied ethics and both the good and bad uses of technology. Data scraping does not only concern possible infringements of rights, e.g., the rights of data owners and website developers, but also several uses of technology that are arguably beneficial. On the other hand, attention is drawn to the current state-of-the-legal-art. In particular, the focus shall be both on the US and Europe which, while simplifying a more complex global scenario, provide a quite comprehensive overview of the array of legal protections against, e.g., screen scraping and allow to make our findings and recommendations equally potentially relevant to other countries. Landmark rulings across multiple jurisdictions illustrate the key legal claims brought against data scrapers and how such claims, however, often fall within the loopholes of the law. Drawing on this basis, in the final part of this paper, a list of open issues that will need further consideration is under scrutiny, namely the pros and cons of the technology, the rulings of the Courts and the persisting legal uncertainty. Despite different approaches and opinions among scholars and jurisdictions, the aim is to cast light on some common trends in the legal domain that offer a guide to the normative troubles of the field.

1. The ethics of data scraping.

Scraping has many useful applications, and it is often used by individuals serving the public interest. Many widespread uses of data scraping benefit both data hosts and scrapers. Scraping services allow users to find the information they seek more easily. Journalists use scraping technology to gather and analyze massive chunks of statistical data. Scholars employ scraping technology for their academic research. Popular search engines, such as Google and Bing, crawl the web and scrape web pages to provide search results. Since most website traffic often comes from search engines, data hosts do not oppose access to most crawling bots, given the overwhelming benefit they derive. In the case of metasearch engines, data scraping enables them to extend the gathering of data and information – and to compare e.g., product and price information from various sources – exempting users from visiting and checking multiple webpages or search engines. Further possible uses of the technology include tracking companies' reputation or aggregating news and other content on curated websites.[2] However, despite these beneficial applications, scraping technology can also be used for malicious purposes, such as spamming email accounts, causing website crashes,[3] or setting scams.[4]

[1] An overview of legal issues arising from data scraping is provided also in J Ciani Sciolla, 'The normative challenges of data scraping: legal hurdles and steps forward' (2023) 16 i-lex Riv Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale: i-vi, working as an introduction to a special issue entirely devoted to study the many legal facets of the phenomenon.

[2] A Sellars, 'Twenty Years of Web Scraping and the Computer Fraud and Abuse Act' (2018) 24 BU J Sci & L Tech, 381-382.

[3] M Boulanger, 'Scraping the Bottom of the Barrel: Why It Is No Surprise That Data Scrapers Can Have Access to Public Profiles on Linkedln' (2018) 21 Smu Sci & Tech L Rev,77-78.

[4] K Collier, 'Why Cybercriminals Looking to Steal Personal Info Are Using Text Messages as Bait'. NBC NEWS, 6 May 2021.

Scraping may also be parasitic: scrapers can benefit from the exclusion or detriment of data hosts; they can undercut a website's revenue by republishing scraped data without requiring users to view supporting advertisements; moreover, scrapers can attain their own ad revenues, viewers, and customers by taking content from another data host. Scraping may also affect the protection of fundamental rights by collecting personally identifying information with serious privacy implications. For example, the technology is problematically employed in the so-called 'mugshot gallery': by displaying the photos of arrested people, scrapers monetize them in various ways, e.g., charging individuals to have their images removed.[5]

Against this backdrop, scholars often insist on both 'beneficial' and 'harmful' uses of scraping,[6] also referring to data scraping as a phenomenon 'intertwined with both good and evil' and with 'paradoxical two-sided effects'.[7] Arguably, the troubles with scraping do not regard the technology as such. Data scraping is a form of copying that simulates the human processing of copying and pasting texts or images from a webpage. In general terms, scholars have extensively discussed the 'ethics of copying'.[8] Copying is essential for individual and social learning processes, cultural development, and economic success.[9] Copying enables democratization processes by providing access to cultural goods and relevant information. Mental activity seems to be a form of copying as well. Therefore, it is simply wrong to assume that copying should be regarded as something immoral.[10] Rather, attention should be drawn to how copying fits into a broader system of values that scholars have explored in such fields as philosophy of art and technology, philosophy of law and ethics, legal theory and media studies, art history and literary theory, or sociology.[11] Drawing on this basis, it is thus evident that the problem does not regard any scraping as such. The assumption is confirmed by the paradoxical effects that would follow a ban on technology. The overall prohibition of web scraping would increase the barriers-to-entry by prescribing licensing deals for new entrants. In addition, every ban could negatively impact competition and hence foster monopolistic positions of incumbents.[12] Correspondingly, what is at stake is not the 'morality of scraping' but rather how to strike a fair balance between such web practices and a broader system of values, such as the rights and interests protected under legal provisions[13]. After all, the activity of

[5] EK Lee, 'Monetizing Shame: Mugshots, Privacy, and the Right to Access' (2018) 70 Rutgers U L Rev: 566, 569; A Rostron, 'The Mugshot Industry: Freedom of Speech, Rights of Publicity, and the Controversy Sparked by an Unusual New Type of Business' 90 Wash U L Rev,1323-1324.
[6] MF Din, 'Breaching and Entering: When Data Scraping Should Be a Federal Computer Hacking Crime' (2015) 81 Brooklyn L Rev, 412-415.
[7] L Qian, J Tao, 'Rethinking Criminal Sanctions on Data Scraping in China Based on a Case Study of Illegally Obtaining Specific Data by Crawlers' (2020) 4 China Leg Science,136-158.
[8] R De George, 'Information technology, globalization and ethics' (2006) 8 Ethics and Inf Tech:29, 40; DH Hick, R Schmücker (Eds) *The Aesthetics and Ethics of Copying* (Bloomsbury Publishing, 2016).
[9] U Pagallo, 'The Troubles with Digital Copies: A Short KM Phenomenology' In *Digital Rights Management: Concepts, Methodologies, Tools, and Applications* (Hershey, IGI Global 2013) 1379, 1394.
[10] S Bringsjord, 'In Defense of copying' (1989) 3 Public Aff Quart, 1-9.
[11] Hick and Schmücker (n 8).
[12] M Husovec, 'The end of (meta) search engines in Europe?' (2014) *Max Planck Inst for Innov and Comp Res Pap Series*, 14-15.
[13] V Krotov, L Johnson and L Silva, 'Legality and Ethics of Web Scraping' (2020) Communications of the Association for Information Systems, 47.

copying in itself acquires different moral connotations according to the context. Therefore, an ethical approach is necessary to discern good from bad uses of technology, especially considering the troubles of the law with the very distinction between legitimate and illegitimate web scraping practices. The focus of the following parts of this paper is on such current legal troubles and how ethics is relevant for the assessment and further development of current legal standards.

2. The law of data scraping.

The 'ethics of copying' shall be tested against the myriad legal problems brought about by data scraping. No statute specifically addresses the challenges of technology. Multiple jurisdictions – e.g., the US and EU national courts case law, under scrutiny in this paper – have followed a wide range of different paths. They regard legal issues on (i) unfair competition of metasearch engines; (ii) contractual liability as regards the website terms and conditions and whether they are binding for the scraper; (iii) non-contractual liability, with critical differences between common law and civil law jurisdictions; (iv) copyright; (v) sui generis rights on databases; down to, (vi) personal data, or data which is kept secret. Each of these cases poses thorny legal issues of its own. Let us start the legal analysis of this part of the paper with the lenses of tort law on unfair competition. The notion is traditionally intertwined with ethical considerations on whether a defendant may have violated 'honest practices in industrial or commercial matters' (art. 10 bis TRIPs agreement).

2.1. Unfair competition of metasearch engines, or the Ryanair saga.

In the introduction, we mentioned the battle of website developers against scraping developers, such as popular metasearch engines or search aggregators that hinge on third-parties' data. We noted that data owners, or data holders, often deem screen scraping as illegitimate. For example, Ryanair, the low-cost airline company headquartered in Ireland, lodged multiple parallel lawsuits against online travel agencies in the early 2010s. The aim was to stop the scraping of information from Ryanair's website that allowed such online travel agencies to sell flight tickets through their own services. In December 2013, the Court of Justice of the European Union handed down the *Innoweb* ruling. The Court labeled the actions of the metasearch engines as 'nearly parasitic', e.g., letting users parse through multiple databases of car ads listed on third-party sites (para. 48). In addition, Justices in Luxembourg held that metasearch engines likely infringe the database right of the indexed website, assuming that such right represents a protectable subject matter of its own.

It is noteworthy, however, that several national courts in Europe did not follow suit. For example, the German Federal Supreme Court, in *Ryanair v. Vtours*, established that a metasearch engine that carries out a booking on behalf of the consumer, or even under its own name (integrated booking), does not necessarily engage in an act of unfair competition. Likewise, in *Ryanair v.*

Viaggiare,[14] the Italian Supreme Court stated that scraping datasets is not illegal per se, except for possible infringements of intellectual property rights (IPRs).[15] The same holds true for the Grand Instance Court in Paris and the Spanish Court of Appeal, which established that travel agencies did not incur in the tort of parasitic unfair competition since their operations did not affect the normal functioning of the market or alter the market's competitive structure. Furthermore, the business of such online companies even brought Ryanair new customers and was overall beneficial for both the users and the market. The opposite views of the EU Court of Justice and several national jurisdictions in Europe are not unique to the old continent. Further cases on web scraping in different US Circuits have, in fact, seen opposite conclusions on how to interpret the Computer Fraud and Abuse Act ('CFAA') regarding data scraping practices. The following subsections examine this disagreement in detail, distinguishing between contractual and non-contractual liability of scraping developers and between civil and common law jurisdictions.

2.2. Contractual liability: Are the website terms and conditions binding for the scraper?

Data holders' claims against web scrapers involve both contractual obligations and non-contractual duties. Under the first scenario, a website's terms of service, or 'ToS' may prohibit scraping[16]. This was the case with the Ryanair's ToS. They allowed screen-scraping only for non-commercial purposes, thus excluding flight ticket sales in competition with Ryanair. Since there is no statute – as far as we know – that specifically targets data scraping, plaintiffs have intended to challenge the behavior of scraping developers on contractual basis. Since most websites' ToS prohibit the automated collection, scraping, use, and reproduction of data without permission, the question is how courts may interpret these terms, in particular, whether such ToS should be conceived of as enforceable contracts[17].

Courts and scholars usually distinguish three types of online contracts: (i) clickwrap, i.e., the user must affirmatively click 'I agree' before accessing the website; (ii) scrollwrap, i.e., the user must scroll through the contract and click 'I agree'; and, (iii) browsewrap, i.e., the user agrees to the contract by using the website.[18] Courts generally find clickwrap and scrollwrap agreements enforceable because, at some point during the registration or use of the website, users check a box to acknowledge they agree to the terms. However, since, most of the time, scraping activities do not require any consent to ToS – apart from browsewrap contracts or similar – the enforceability of ToS is problematic. All in all, both in Europe and in the US, courts have dismissed breach of contract claims against web scrapers when there is no evidence that

[14] Cass Civ 18.12.2018 n 2289, 2290.
[15] FE Beneke Avila, 'The German Federal Supreme Court's judgment in Booking.com as a case study of the limitations of competition law' (2022) IIC Int Rev IP and Comp L,1374.
[16] A Quarta, MW Monterossi, 'Web Scraping: A Private Law Perspective' (2023) 16 i-lex Riv Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale, 46-52.
[17] M Borghi, S Karapapa, 'Contractual Restrictions on Lawful Use of Information: Sole-Source Databases Protected bythe Back Door? ' (2015) 37 EIPR, 505-511.
[18] E Canino, 'The Electronic "Sign-in-Wrap" Contract' (2016) 50 U.C. Davis L. Rev, 539-541.

the link to the terms of use is displayed among all the links of the site, at least, at the bottom of the page as most sites on the internet.[19] Moreover, web scrapers are not accountable when they have no actual or 'constructive knowledge' about the terms and conditions of the website.[20] The Grand Instance Court in Paris found that Opodo was not bound by the terms of service on the Ryanair website; as much as the Spanish Supreme Court concluded that accessing and visiting the Ryanair website – free to anyone who types the URL address – does not entail any consent to enter into a contract. The Italian Supreme Court ruled along the same lines, pointing out that, although the scraper carried out something not allowed by Ryanair's ToS, the scraper never consented to such ToS, and no contract violation would thus exist. However, we should not jump to conclusions. Other cases show that plaintiffs can demonstrate the 'actual knowledge' of their counterparties through cease-and-desist letters. For example, in *Ryanair Ltd v Billigfluege.de GmbH*, Ireland's High Court ruled that Ryanair's 'click-wrap' agreement is legally binding since the hyperlink was plainly visible, putting the burden of agreeing to the ToS in order to gain access to the online services on the user. The ruling of the Irish Court over the Irish company – and against a German travel agency – seems at odds with most jurisdictions in the old Continent. This legal uncertainty has suggested that data owners, or data holders, such as Ryanair, complement their contractual claims with further claims of non-contractual liability.

2.3. Non-contractual liability: Common law versus civil law approaches toward data scraping.

Non-contractual liability issues of data scraping highlight the differences between common law and civil law. In Europe, most of the time, courts have to decide whether the scraper infringed exclusivity rights over the scraped data: intellectual property rights are the natural legal framework for such cases in EU law. Therefore, the focus of EU lawyers is on whether scraping extracts data that is protected as a database. Other laws, e.g., data protection law, competition law or the law governing the use of public sector information, may also be relevant, depending on the features of the scraped data. In the US, the 'thin' protection provided to databases by the so-called 'copyright's database-sized gap' has recommended website owners seek remedies in criminal and tort law. In particular, discussions have often revolved around the CFAA from 1986, which punishes 'whoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information'.

---

[19] In *QVC Inc. v. Resultly LLC*, No. 14-06714 (E.D. Pa., filed 24 November 2014) the court ruled that the ToS should be brought to the users' attention in order for a browse wrap contract or license to be enforced. This is not the case when the ToS link is displayed among all the links of the site, at the bottom of the page as most sites on the internet.

[20] For example, in *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2D 927, 96 U.S.P.Q. 2d 1798 9 (E.D. Va. 2010), a federal court in the Eastern District of Virginia dismissed a breach of contract claim against a web scraper because the plaintiff's T&C was a browsewrap agreement and the plaintiff had not 'pled sufficient facts to plausibly establish that defendants Eventbrite and Foley were on actual or constructive notice of the terms and conditions posted on Cvent's website.'; the court reached a similar conclusion in *Alan Ross Machinery Corporation v. Machinio Corporation*, No. 1:2017cv03569 - Document 31 (N.D. Ill. 2018).

For years, courts have debated the meaning of the formula 'without authorization' under the CFAA, i.e., whether the CFAA is best understood as 'an anti-intrusion statute' or a 'misappropriation statute'.[21] In 2019, the Ninth Circuit issued its opinion in *hiQ Labs, Inc. v. LinkedIn Corporation,*[22] in which the key question was to determine whether a computer's gates were up or down. The Court interpreted the CFAA as an anti-intrusion statute prohibiting unauthorized access and what is traditionally conceived as 'hacking'.[23] Unauthorized access occurs 'when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements'. Public websites like LinkedIn, however, permit public access to their data, such as available LinkedIn member profiles, so that the decision of the Ninth Circuit was that 'a user's accessing that publicly available data will not constitute access without authorization under the CFAA'. In light of this ruling, not only have several scholars argued that the CFAA is ill-suited for tackling web scraping cases,[24] but also, far from relying on the protection of the CFAA rules, plaintiffs have embraced further legal strategies under US tort law, so that web scraping practices would entail either common law misappropriation, i.e., the 'hot news' tort;[25] unjust enrichment;[26] conversion;[27] or trespass to chattel.[28] The 'hot news' tort originated with the seminal Supreme Court case *INS v. AP*, in which a press agency copied the facts reported in the news bulletins of its competitor. Despite facts in the news being considered uncopyrightable information in the public domain, the Supreme Court recognized that these facts were 'the result of organization and the expenditure of labor, skill, and money'. Correspondingly, *INS* was 'endeavoring to reap where it has not sown'.[29] The 'hot news' tort thus applies to cases of web scraping and protected websites according to four conditions: (i) the plaintiff generates or collects information at some cost or expense; (ii) the defendant's use of the information constitutes free-riding on the plaintiff's costly efforts to generate or collect it; (iii) the defendant's use of the information is in direct competition with a product or service offered by the plaintiff; and, (iv) the ability of other parties to free-ride on the efforts of the plaintiff would shrink the incentive to create the product or service, whose existence or quality would then substantially be threatened.[30]

The problem with the 'hot news' tort approach, however, is that it only protects time-sensitive information, leaving a wide variety of databases unprotected from scraping. To prevent this lack of protection, two further state law torts, i.e., conversion and trespass to chattel, may provide some

[21] M Addicks, 'Van Buren v. United States: The Supreme Court's Ruling on the Fate of Web Scraping - "Access" to Discovery or Detention?' (2022) 24 Tul J Tech & Intell Prop, 161.
[22] 938 F.3d 985, 995 (9th Cir. 2019).
[23] Boulanger (n 3).
[24] JE Christensen, 'The Demise of the CFAA in Data Scraping Cases' (2020) 34 Notre Dame J.L. Ethics & Pub. Pol'y, 529.
[25] See e.g. *Allure Jewelers, Inc. v. Ulu*, No. 1:12CV91, 2012 WL 4322519 (S.D. Ohio 25 September 2012).
[26] See e.g. *Snap-on Bus. Sols. Inc. v. O'Neil & Assocs, Inc.*, 708 F. Supp. 2D 669, 680-82 (N.D. Ohio 2010); *ShopLocal LLC v. Cairo, Inc.*, No. CIV.A. 05 C 6662, 2006 WL 495942, at *3 (N.D. Ill. 27 February 2006).
[27] See e.g. *QVC, Inc. v. Resultly,* LLC, 159 F. Supp. 3D 576(E.D. Pa. 2016).
[28] See e.g. eBay, *Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1065-71 (N.D. Cal. 2000).
[29] *Int'l News Serv. v. Associated Press*, 248 U.S. 215, 247 (1918).
[30] *Nat'l Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841, 852-53 (2d Cir. 1997).

remedy. Liability for trespass to chattels traditionally concerns the intention to take or intermeddle with a chattel possessed by someone else. Since the 1990s, this tort has been applied to cases involving devices that automatically overuse phone and email networks and diminish their functionality. The tort has been used in scraping cases as well. To establish a trespass to chattels claim, data hosts have to show that they were dispossessed of their chattel, that their chattel's condition, quality, or value was impaired, or that they were 'deprived of the use of their chattel for a substantial time.' In the case of conversion, the difference with the trespass to chattels claim consists in a more serious deprivation of the owner's rights, so that 'an award of the full value of the property is appropriate.'

These torts and the CFAA can be understood as 'quasi-IP' regimes because they serve to protect proprietary interests which are not covered by the law of copyright. To demonstrate conversion or trespass to chattel, plaintiffs must meet a stringent standard regarding the proof of actual injury to their computer systems. In many cases, however, scraping will have a negligible impact on the plaintiff's servers, making these claims unlikely to succeed. By considering the drawbacks of US regulations, would the EU sui generis right on databases offer better protection?

2.4. Copyright over data and datasets.

The question of whether and to what extent databases should be protected by the law concerns two potentially conflicting goals: that of providing adequate incentives for the continued production of such databases, and that of ensuring public access to the information they contain. In Europe, the assumption is that the disparity of the fixed costs needed to create a database and the marginal costs to copy or access it, necessarily makes it an *ad hoc* intellectual property right, i.e., Directive 96/9 on the legal protection of databases. The protection entails an exclusive right that enables the database maker to charge, for a limited time, a price superior to the marginal cost for the use of its database and to select other market participants who can take advantage of such database as licensees, thus boosting the database production.

Things have gone differently in the US.[31] Based on the 1998 US Copyright Office's report on legal protection for databases, Congress dismissed any proposals for establishing a new form of database right on the grounds that copyright law should not favor the protection of factual data unless facts have been selected, coordinated, or arranged in an original way. Therefore, the threshold is not satisfied when the setting up of a database is determined by technical considerations, rules or constraints, which leave no room for creative freedom.[32] The US Supreme Court has expressly rejected the 'sweat of the brow' theory, under which copyright could be granted just as 'a reward for the hard work that went into compiling facts'. In its seminal case, *FeistPublications*

[31] JC Ginsburg, 'Copyright, Common Law, and Sui Generis Protection of Databases in the United States and Abroad' (1997) 66 U Cin L Rev, 153-157.
[32] Case C-604/10, *Football Dataco Ltd vs. Yahoo! UK Ltd* (CJ, 1 March 2012).

Inc. v. Rural Telephone Service Co.,[33] Justices in Washington denied copyright protection to a telephone directory because the latter was a mere collection of unoriginal facts, regardless of whether immense efforts were needed to compile the directory. The US District Court of the Central District of California confirmed this view in *Ticketmaster v. Tickets.com,* [34] where Tickets.com employed an electronic web crawler that reviewed Ticketmaster's website and extracted the information on events for which Ticketmaster offered the sale of tickets. The court reasoned that 'the primary star in the copyright sky... is that purely factual information may not be copyrighted.'

In addition, although data scraping may amount to *prima facie* copyright infringement, it could still fall under copyright exceptions, limitations, or fair use defenses. In *Perfect10 v. Amazon.com,*[35] for example, Google was sued under copyright law for scraping thumbnail images of a magazine's covers as a part of the Google Image Search. However, the Ninth Circuit found Google's scraping to be fair use because it 'provided a significant benefit to the public' and was highly transformative.

In Europe, where copyright law does not include a fair use clause, scraping may be lawful under a series of 'exceptions.' They regard (i) the exception for temporary copies (Art. 5.1 Directive 2001/29); (ii) the text and data mining exception introduced by Art. 3 and 4 of the Directive on Copyright in the Digital Single Market (CDSM);[36] down to Art. 1.6 of Directive (EU) 2019/1024 on open data and the re-use of public sector information. According to this latter directive, 'the right for the maker of a database provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of documents or to restrict re-use beyond the limits set by this Directive'. Leaving aside the interpretation of these provisions, it is noteworthy that some scholars are pessimistic about the possibility of anyone who is not a research and cultural organization acting for research purposes lawfully scraping data in Europe.[37] Yet, in Italy, the Court of Rome has considered the scraping of the state rail-transport operator's data conducted by a web aggregator lawful on the basis of Art. 7(1) of the open data directive.[38] In light of these 'exceptions', that protect web scrapers activities, the focus is next fixed on the corresponding general rules.

---

[33] *Feist Publ'ns, Inc v. Rural Tel Serv Co.*, 499 U.S. 340, 345 at 361 (1991).

[34] *Ticketmaster Corp. v. Tickets.com, Inc*, 2003 WL 21406289 (CD Cal. 2003). See S O'Reilly, 'Nominative Fair Use and Internet Aggregators: Copyright and Trademark Challenges Posed by Bots, Web Crawlers and Screen Scraping Technologies' (2007) 19 Loy Consumer L Rev, 273.

[35] 508 F.3d at 1155-56 (9th Cir. 2007).

[36] The goal of Art. 3 is to introduce a mandatory exception under EU copyright law which exempts acts of reproduction (for copyright subject matter) and extraction (for the Sui Generis Database Right) made by research organisations and cultural heritage institutions in order to carry out text and data mining for the purposes of scientific research. Art. 4 mirrors Art. 3 with one major difference: it is available to any type of beneficiaries for any type of use but can be expressly reserved by rightsholders – in other words it may be the object of 'opt-out' or 'contract-out'. C Gallese, 'Web scraping and Generative Models training in the Directive 790/19' (2023) 16 i-lex Riv Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale, 1-13.

[37] T Margoni, M Kretschmer, 'A deeper look into the EU Text and Data Mining exceptions: Harmonisation, data ownership, and the future of technology' (2021) CREATe Working Paper, 7.

[38] J Ciani Sciolla, *Il pubblico dominio nella società della conoscenza. L'interesse generale al libero utilizzo del capitale intellettuale comune* (Giappichelli 2021), 221.

2.5. The database sui-generis right.

In EU law, the assumption is that databases shall not be original to be protected. Contrary to US law, Chapter III of Directive 96/9/EC grants a 'sui generis' protection to EU makers of a database, which shows that there has been a qualitatively and/or quantitatively substantial investment in either the obtaining, the verification or the presentation of the contents. In particular, the database creator is entitled to prevent extraction and/or re-utilization of both the whole database or a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database (Art. 7). If the requisites are met, the protection is granted automatically for 15 years starting either from the creation date or from the day in which the database was first made publicly available.

Since the early days of the database sui generis rights, several plaintiffs have progressively invoked this law against the data scraping of metasearch engine operators. Consequently, courts must first check whether the scraped website contains a database according to the definition of Art. 1.2 of the database directive,[39] whereas Art. 3.2 clarifies that the protection does not extend to the contents of the database. On this basis, it is worth mentioning that in one of the multiple lawsuits brought forth by Ryanair in Europe, the Spanish Supreme Court ruled that Ryanair does not have a collection of independent data under the database provisions, but rather, rights upon a software that generates the information requested under the parameters introduced by the user, i.e., a software that provides the best price for the flights users are looking for, considering a range of variable factors.

The ruling of the Spanish Supreme Court, however, has been contradicted by other courts. For example, the Italian Supreme Court[40] and the Regional Court of Hamburg[41] have both declared that Ryanair does have a database under Art. 1.2 of the 1996 Directive. The assumption begs two further questions concerning the main legal thresholds that trigger the protection of a database: (i) substantiality of the investment; and (ii) substantiality of the extraction.

2.5.1. Substantiality of the investment.

The first threshold is defined as the 'qualitatively and/or quantitatively substantial investment in either the obtaining, verification or presentation of the contents' (Art. 7(1) of the database directive). According to the CJEU, what matters is that 'the obtaining of those materials, their verification or their presentation [...] required substantial investment in quantitative or qualitative terms, which was independent of the resources used to create those materials.' The burden to prove all the facts substantiating the relevant investment falls upon the person or company claiming protection.

---

[39] 'For the purposes of this Directive, "database" shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.'

[40] Above n 14.

[41] *Ryanair v Cheaptickets* (26 February 2010).

EU national courts have interpreted this requirement in different ways. For example, the Grand Instance Court in Paris found no infringement of a database right as Ryanair did not prove to have made substantial investments necessary to pretend such protection. Likewise, as mentioned in the previous section, the Spanish Supreme Court concluded that Ryanair's substantial investment was not directed to protect data but to create a software that generates information under the user's search query parameters.[42] Similar arguments and outcomes are stressed in *Ryanair v. eDreams,*[43] another legal case that ended with a dismissal of Ryanair's claims. On the contrary, the Italian Supreme Court considered that Ryanair's investment can be presumed, although this presumption does not entail that the claims of the Irish company should be deemed substantiated. Against these opposite views, attention should be drawn to the second threshold of the EU database directive.

2.5.2. Substantiality of the extraction.

The second threshold requires that the acts to extract or reuse data via scraping concern the totality or a substantial part of the database. Extracting or reusing data in a limited or partial way – i.e., in both quantitative and qualitative terms – is thus implicitly considered admissible, regardless of any rightsholder's authorization. Also, scraping is lawful when those acts are systematically and repeatedly carried out but involve non-substantial parts of the information contained in the database, i.e., the so-called 'diachronic extraction.' Vice versa, no extraction or reuse is allowed insofar as such acts require operations that conflict with the normal use of the database or cause excessive harm to the legitimate interests of its creator(s). Accordingly, courts are requested to establish whether the extraction is 'substantial enough' or – in the event of diachronic extraction – the latter harms the legitimate interest of the database maker.

Interestingly, these requirements are also taken into account by US Courts, although for different purposes. On the basis of the substantial copying requirement, courts have to determine whether competition is fair or unfair, that is, whether scraping triggers beneficial dissemination of information or harmful free-riding. The Eleventh Circuit, for instance, held that scraping is unlawful only when it concerns a substantial amount of data, such that 'the block of data that the defendants took was large enough to constitute appropriation of the [d]atabase itself'.[44]

In order to assess the substantiality of the extraction and the related harm, some jurisdictions, e.g., Italy, inspect the logs of the scraped website. In a case where the number of logs corresponded roughly to 30% of the total daily accesses—a figure defined as 'non impressive'—the Court of Rome established that there was no extraction of a substantial part of the database.[45] However, the Court pointed out that such logs were legitimate only if they represented

[42] Tribunal Supremo, *Ryanair v Atrapalo*, Case No. 572/2012 (2012).
[43] Curtea de Apel Barcelona, R*yanair v Vacaciones Edreams* (2009).
[44] See e.g. *Compulife Software Inc v. Newman*, 959 F.3d 1288, 1314 (11th Cir. 2020).
[45] District Court of Rome, *Trenitalia S.p.a. v GoBright Media Ltd* (5 September 2019).

forms of contingent accesses and periodic and selective acquisitions of data, each of which following a specific search query by a user.

In the case of diachronic extraction, Italian courts have made it clear that the harm to the legitimate interest of the database maker should consist of something more than just the loss of profit or income that derives from the absence of a license and subsequent lack of payment of license fees. Since metasearch engines are considered pro-competitive businesses, the harm cannot result in any loss of revenues deriving from the reduction in the volume of the traffic on the scraped website. Instead, harm should be deemed unjust only when scraping impairs the database's normal operativity because of the overload caused by the scraper's traffic. This was the argument at stake in *QVC Inc. v. Resultly*, where the e-commerce site QVC claimed that the shopping aggregator 'excessively crawled' the QVC's retail site – allegedly sending 200-300 search requests to the QVC's website per minute, sometimes up to 36,000 requests per minute – so that the website crashed for two days, resulting in lost sales for QVC.

Most of the time, however, scraped companies do not lose anything as a result of these activities and, therefore, no proof of tangible harm can be demonstrated. In general terms, diachronic data extraction is far more difficult to challenge than synchronic extraction, which is not necessarily good news for data holders. Indeed, most scraping activities are diachronic.

2.6. The nature of scraped data: personal, public or secret.

The law applicable to scraping operations may vary depending on the nature of the scraped data. Such data can be personally identifiable information, publicly available information, or data and information kept under secret, e.g., trade secrets. Each case presents its specificities, which are examined separately in the following subsections.

2.6.1. The scraping of personal data.

Over the past few years, consumer data privacy legislation has gained traction in the US. The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), for instance, regulate the collection of consumers' personal data and the sharing of such data with third parties.[46] However, it seems fair to admit that no currently proposed or enacted privacy statute adequately protects publicly available personal information. All of this is exempted, making it fair game to scrape, use, share, or sell such personal data. Therefore, US privacy laws have not been the frequent subject of web scraping litigation. Few scholars have indeed addressed the privacy implications of scraping publicly available personal information.[47]

On the other hand, the EU has much more stringent laws on the scraping of personal data, and EU law even imposes fines on web scrapers who violate

[46] W Barfield, U Pagallo, *Advanced Introduction to Law and AI* (Elgar 2020).
[47] G Xiao, 'Bad Bots: Regulating the Scraping of Public Personal Information' (2021) 34 Harv J L & Tech:702; AM Parks, 'Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Data Scrapers' (2022) 120 Mich L Rev, 913.

provisions of data protection. The legal troubles of *Clearview AI* illustrate this point[48]. The company has been embroiled in multiple lawsuits stemming from its conduct in scraping billions of facial images from the Internet and creating a biometric database that allows users to immediately identify a member of the public merely by uploading a person's image to the database.[49]

In April 2020, the French data protection authority (CNIL) published guidance on the lawful scraping of personal data for direct marketing purposes. Although contact information may be available on publicly accessible websites, the individuals who posted the information do not reasonably expect to have it scraped for 'prospecting'. Therefore, according to CNIL, such personal data cannot be re-used for marketing without the consent of the data subject obtained prior to any reuse. The CNIL clarifies that accepting the ToS – meaning that the individual accepts to receive marketing communications – is insufficient, as it is not specific to make web scraping of personal data lawful.

On 24 August 2023, twelve data protection authorities from around the world published a joint statement outlining the key privacy risks associated with data scraping taking place on social media as well as the steps that both websites and individuals should take to minimize such risks and meet regulatory expectations.[50]

In general terms, the opinion of courts and regulators at the EU level suggests that web scraping involving the collection of personal data is unlawful if it does not comply with the principles and provisions of the general data protection regulation, the GDPR.[51]

2.6.2. The scraping of data as an essential facility.

Antitrust issues are often at the core of web scraping litigation. For example, antitrust issues with data control were at the core of the Ryanair saga in Europe. The Italian Supreme Court, among others, found that Ryanair abused its dominant position in the downstream market for the provision of information for its own flights (sole source) by refusing access to an essential facility it owns (data about flight schedules and prices). Similar problems may arise in the US as well. A monopolist operating a public website could be liable under the 'refusal to deal' doctrine under Section 2 of the Sherman Act for restricting data access by means of exclusionary data scraping prohibitions.[52]

In *hiQ Labs, Inc v LinkedIn Corp*, the Ninth Circuit questioned the legitimacy of LinkedIn's data scraping prohibition, explaining that 'if companies like LinkedIn, whose servers hold vast amounts of public data, are permitted selectively to ban only potential competitors from accessing and using that

[48] F Lala, 'Data collection via web scraping: privacy and facial recognition after Clearview' (2023) 16 i-lex Riv Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale, 34-44.
[49] I Neroni Rezende, 'Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective' (2020) 3 *New Jour of Eur Crim L*,375-389.
[50] Joint Statement on data scraping and the protection of privacy, 24 August 2023.
[51] U Pagallo, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (2017) 3 Eur Data Prot L Rev, 36.
[52] 15 USC § 2 provides that '[e]very person who shall monopolize, or attempt to monopolize, or combine or conspire... to monopolize...shall be deemed guilty of a felony.' See I Drivas 'Liability for Data Scraping Prohibitions under the Refusal to Deal Doctrine: An Incremental Step toward More Robust Sherman Act Enforcement' (2019) 86 U. Chi. L. Rev., 1901.

otherwise public data, the result - complete exclusion of the original innovator in aggregating and analyzing the public information - may well be considered unfair competition'. On this basis, the court dismissed LinkedIn's proffered justifications that the prohibition served its users' privacy because the company shared its users' data with third-parties for commercial purposes. Likewise, LinkedIn could not persuasively claim the prohibition was justified as a measure against free riding because the company could not claim ownership of the data and users clearly intended to make their profiles publicly accessible. The Ninth Circuit dismissed LinkedIn's defense because giving companies 'free rein to decide... who can collect and use data... risks the possible creation of information monopolies that would disserve the public interest.'.

2.6.3. The scraping of data kept secret.

Web scraping may also concern data protected as a trade secret. In EU law, the definition and protection requirements are set up in Directive 2016/943/EU (Trade Secrets Directive) on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Such provisions are very similar to the Uniform Trade Secrets Act ('UTSA') in US law. Both statutes are modeled on Art. 30 of the TRIPS Agreement and require both the existence of a trade secret and its misappropriation.

As regards the existence of such trade secret, it hinges on three conditions: (i) a trade secret must not be generally known to or readily ascertainable by others; (ii) the owner must have taken reasonable measures to keep such information secret; and, (iii) the information must originate independent economic value from the fact of being secret. The critical point that follows as a result is whether the use of data scraping technologies to automatically extract the information contained in a website makes this information 'readily accessible' and, hence, not so secret. Information is considered readily accessible if it is not generally known but can be obtained by otherwise fair means without considerable effort and expenditure of time, effort, expense and/or skill. In both EU and US law, courts do not doubt that a database may be considered a trade secret. For example, the Court of Milan, Italy, specified that the commercial value of secret information does not concern the information as such, but rather, the way in which such information might be processed by 'dynamic technologies'. In fact, the Court stressed that the status of the information as a potential trade secret should be assessed in relation to the configuration and combination of the dataset as a whole and not just its individual elements in isolation. This is relevant because, after a search query, only individual elements are disclosed to the public, not the whole database.

Similar arguments are at work with the Eleventh Circuit's ruling in *Compulife.*[53] Although parts of a database can be known by the public, the database as a whole can be secret so that compilations of information are protectable even when each piece of information is under public knowledge. In the phrasing of the Restatement (Third) of Unfair Competition § 39, 'it is the

[53] *Compulife Software, Inc v Rutstein*, No. 9:16-CV-80808-JMH, 2018 WL 11033483, at *18-22 (S.D. Fla. 12 March 2018).

secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation or integration of the individual elements'. Accordingly, a website's decision to place its database on the internet and allow public access to individual pieces of data does not mean that the website failed to take 'reasonable measures to keep [its database] secret.' The Eleventh Circuit's assumption is that the data holder had a reasonable expectation that others would not engage in massive, automated plagiarism. In other words, a trade-secret owner's failure to place a usage restriction on its website does not exclude the violation of its trade secrets.

This conclusion seems reasonable due to the state-of-the-art of technological protection measures. The ability to scrape publicly available content, register fake user accounts for malicious bots, or pass valid HTTP requests from randomly generated device IDs and IP addresses makes traditional rule-based security measures ineffective against sophisticated scraping activities. Web application firewalls are not designed to detect real-time automated threats and struggle to recognize most of today's sophisticated bots. This is why new solutions for bot detection or anti-crawler protection have been developed to identify a visitor's behavior that shows evidence of web scraping in real-time, automatically blocking malicious bots while maintaining a smooth experience for real human users. DataDome,[54] for example, compares in real-time every site hit with an in-memory pattern database to decide, through a machine learning algorithm, whether to grant access to the webpages. However, to correctly identify fraudulent traffic and block web scraping tools, a bot protection solution must be able to analyze both technical and behavioral data to set up a list of trusted partner bots, a task that may be very invasive.

Against this sort of technological cat-and-mouse game, we may thus wonder about the 'reasonable steps' that trade secret owners shall take to protect their rights. After all, in EU trade secrets litigation, one of the most common defenses is that no trade secret exists because the claimant failed to take the reasonable steps necessary to keep the information undisclosed. This defense has been successful in 59% of the instances considered in a recent empirical work.[55] Although the notion of 'reasonable steps' is generally subject to a case-specific analysis, it is arguable that – according to the EU courts – some measures that control access to and use of secret information should exist to protect such trade secrets.

Yet, in addition to the 'existential conditions' for any trade secret, we have to further consider the unlawful or improper means of web scraping to access trade secrets, namely, their misappropriation under Art. 30 of the TRIPS Agreement. The main legal issue revolves around the acquisition of such secrets by legal conduct.[56] Indeed, if data scraping activities are not unlawful as such, they may entail a lawful appropriation of the trade secret. In US law,

[54] DataDome. https://datadome.co/ (27 September 2023, date last accessed).
[55] EUIPO, Study on trade secrets litigation trends in the EU. IPR Enforcement case-law collection, 2023.
[56] WE Hilton, 'What Sort of Improper Conduct Constitutes Misappropriation of a Trade Secret' (1990) 30 Idea J L & Tech, 294-296; RG Bone, 'The Still (Shaky) Foundations of Trade Secret Law' (2014) 92 Tex L Rev,1803-1805.

the landmark case is the Fifth Circuit's decision in *E. L du PontdeNemours & Co. v. Christopher*.[57] According to the ruling, '[a]ctions may be 'improper' for trade-secret purposes even if not independently unlawful.' This means that scraping would be improper, although the activity is not per se unlawful or in breach of contract. This approach has been criticized as 'contrary to a basic understanding of trade secret law',[58] because every method of copying trade secrets would be illegal, making the requirement of the 'unlawful acquisition' either redundant or superfluous. In any event, it seems fair to affirm that, so far, applying trade secrecy law to data scraping has proved easier in the US than in EU law.

3. Discussion.

The troubles of the law with the regulation of web scraping activities offer a fruitful case of applied ethics on how to strike a balance between the pros and cons of the technology. We noted that in several cases, e.g., Ryanair's database and software, Courts have reached different, or even opposite, conclusions. Such disagreement may depend on the lack of clear rules or multiple legal cultures and jurisdictions, e.g., civil law and common law. Admittedly, there is no magic bullet to address this uncertainty, and investigations into current practices of scraping are still in progress to get out with more certainties for market operators and data subjects[59]. Yet, it seems reasonable to look for a common (and coherent) normative framework.[60] Drawing on the 'ethics of copying' mentioned in the first part of this paper, we reckon that this normative framework can be fruitfully provided by a coherent moral theory, such as the 'ethics of information'.[61] In our view, this perspective sheds light on both the troubles of the law with web scraping activities and how to ameliorate the current legal framework through the development of standards, namely, norms, values, or principles that can be adopted as the basis of a legal decision, providing thresholds of evaluation that should allow courts and policy makers to assess benefits and risks of technology.[62]

The stance of information ethics can be summed up in accordance with four laws listed to increase moral value. By assuming not only web data but also private actors, individuals, or scraping developers as 'informational entities' on the internet, the laws of information ethics recommend, on the one hand, that any kind of informational entropy – that is, any destruction or corruption of informational objects in the 'infosphere' – is evil because it entails an 'impoverishment of being' and therefore, entropy should not be caused (Law 0); or it should be prevented (Law 1); or removed (Law 2). On the other hand, Law 3 states that 'the flourishing of informational entities as well as the whole

[57] *E I du Pont deNemours & Co v Christopher*, 431 F.2d 1012, cert. denied, 400 U.S. 1024 (5th Cir. 1970).
[58] PJ Toren, 'A Dubious Decision: Eleventh Circuit Finds Scraping of Data from a Public Website Can Constitute Theft of Trade Secrets (Part I)'. IPWATCHDOG, 2 July 2020.
[59] Italian Data Protection Authority, Act 21 December 2023 [doc n 9972593].
[60] U Pagallo, M Durante, 'Three Roads to P2P Systems and Their Impact on Business Practices and Ethics' (2009) 90 J Bus Ethics, 551-564.
[61] L Floridi, *Information Ethics* (Oxford University Press 2013); M Durante, *Ethics, Law and the Politics of Information* (Springer 2017).
[62] L Busch, *Standards. Recipes for Reality* (MIT Press 2011).

infosphere ought to be promoted by preserving, cultivating, enhancing and enriching their properties'.[63] Therefore, regardless of the legal field under scrutiny with the challenges of web scraping, such challenges can be properly summed up with the laws of information ethics according to four different sets of normative issues.

The first set draws attention to all the cases in which web scraping practices arguably create or augment the 'entropy of the infosphere' by spamming email accounts, causing website crashes or setting up scams. Such malicious activities represent an 'impoverishment of the being' and typically fall under criminal law provisions. Those are the 'bad uses' of technology which should not be caused, or vice versa, should be prevented or removed.

The second set of legal issues regards controversial uses of technology that still provoke no harm. Such cases were illustrated with (i) the distinction between synchronic and diachronic extraction of data through web scraping techniques; (ii) sui generis IP rights on databases in EU law with their exceptions; down to, (iii) 'quasi-IP' regimes in US law. Insofar as data owners or data holders are not able to demonstrate that web scraping practices provoke unjust damages, the laws of information ethics on entropy do not apply since there is no harm caused or that should be prevented or removed. In some jurisdictions, e.g., EU data protection law, such harm may be presumed. We noted in section 3.6.1 that reuses of personal data for marketing purposes are lawful only on the basis of a new consent of the data subject before such reuse. Lack of consent suggests, in fact, the creation of informational entropy in the system, e.g., social and technological practices that impinge on the autonomy and self-determination of individuals. This scenario suggests why scholars often stress the limits of US data privacy law also, but not only, regarding the impact of scraping publicly available personal identifiable information.

The third set of legal issues concerns Law 3 of information ethics. There are many beneficial uses of scraping technology, such as scholars employing it for their academic research or journalists gathering and examining huge volumes of statistical data. Such uses likely contribute to the 'flourishing of informational entities as well as the whole infosphere.' Therefore, lawmakers should not only be neutral and accept those scraping practices, but rather, they should preserve, cultivate, enhance, and enrich them.

Last but not least, the fourth set of legal issues is the most controversial since it regards the hard cases of the field. The grey areas of exceptions to the general rules of the law, e.g., EU database law; the contours of the diachronic extraction of data through web scraping technology and whether such practices are at times parasitical, make it difficult to ascertain in general terms the balance that shall be struck between the pros and cons of web scraping, that is, between the 'flourishing of informational entities as well as the whole infosphere' on the one hand and, on the other, the creation of 'informational entropy.' We claim that, in such cases, lawmakers should be neutral, that is, they shall neither prevent the formation of entropy nor preserve and enhance such scraping activities. It will be up to the courts to tackle such hard cases on individual merits. Whether the doctrine of the courts turns out to be

[63] Floridi (n 61).

problematic – from the EU Court of Justice's ruling in *Innoweb* to the US Fifth Circuit's decision in *du PontdeNemours & Co. v. Christopher* – lawmakers could always intervene with their own provisions.

Conclusions.

The paper has hopefully provided an 'anatomy' of the legal challenges of web data scraping, drawing on the four laws of information ethics. The analysis has illustrated the impact of technology on current regulations, stressing the multiple, different, and even opposite opinions of courts and scholars, between civil law and common law jurisdictions, and between claims of scraping developers and web companies. The aim has been to take sides between 'good' and 'bad' uses of technology, revisiting these cases through notions of informational entropy and the flourishing of the infosphere. We stressed the four different ways in which the law should act accordingly. This normative perspective does not mean that we ended up with the magic bullet. On the contrary, attention should be drawn to all the loopholes and grey areas of the law – from the 'diachronic extraction' of web data to the 'exceptions' of EU law – which will require the development of new standards. The conjecture rests not only on disagreements among courts on the protection of databases or the parasitic nature of web scraping activities but also on further developments of technology. Scraping, as much as copying, is here to stay. The law should wisely govern its impact on the 'infosphere'.

Carleo R, 'The AGCOM regulation on "fair compensation": a co-regulation model in search of efficiency / Il regolamento AGCOM sull'"equo compenso": un modello di co-regolazione in cerca di efficienza' (2023) 2 EJPLT, 20 - 55.
DOI: https://doi.org/10.57230/EJPLT232RC

EJPLT
ISSN 2704-8012



The AGCOM regulation on 'fair compensation': a co-regulation model in search of efficiency*

ROBERTO CARLEO
Full Professor of Private Law
Parthenope University of Naples
Barrister

Abstract

The Council of State (nr. 894/24) appropriately removed the decision by which the Lazio Regional Administrative Court (nr. 18790/23) had suspended the AGCOM regulation on fair compensation, thereby allowing an important attempt to experiment with co-regulation not to be interrupted, in order to strike a balance in the area of free dissemination of online newspaper content between the interests of digital platforms, publishers and the public of the users of the information disseminated.

Digital platforms 'over the top' escape the sovereignty of the legislators of individual territorial states, so that, in order to succeed in adopting market regulation, there is a need for a virtuous collaboration of the platforms themselves, in a public-private co-regulation perspective, facilitated by the role of the sector Authorities, in application of the principle of subsidiarity.

*This article was presented at the International Conference "Technology Innovation Law. International Legal Scholars' Jam Session", 8-9. March 2024, Fondazione Einaudi, Rome.
Scientific Committee: Vincenzo Ricciuto (Uni Tor Vergata Roma), Lucilla Gatt (Uni Suor Orsola Benincasa Napoli), Carla Solinas (Uni Tor Vergata Roma), Mariló Gramunt Fombuena (Uni Barcelona).

© The author(s) 2023, 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: digital platforms; fair compensation; co-regulation; self-regulatory codes; regulated autonomy; private regulatory law; principle of subsidiarity.

Summary: 1. Digital platforms *vs.* AGCOM: Meta's appeals against the regulation on fair compensation and Amazon's appeals against the regulation on the organisation and maintenance of the R.O.C. (Register of Communication Operators). - 2. The perplexities raised by the judgement of the Lazio Regional Administrative Court of 12 December 2023, no. 18790 (Meta v. AGCOM), duly reformed by the Council of State (order no. 894 of 11 March 2024): the need for balancing digital services with fun - 3. The fines imposed on Google by the French antitrust authority. - 4. The judgement TAR Lazio 30 October 2023, no. 16069 (Meta v. AGCM and SIAE). - 5. Self-regulation and co-regulation: an opportunity for efficiency of regulatory sources in the digital marketplace necessary and convenient for the platforms themselves.

1. Digital platforms *vs.* AGCOM: Meta's appeals against the regulation on fair compensation and Amazon's appeals against the regulation on the organisation and maintenance of the R.O.C. (Register of Communication Operators).

The Council of State (Order No. 894/24 published on 11 March 2024) reformed the Lazio Regional Administrative Court's ruling (Order No. 18790/23 published on 12 December 2023) insofar as, by upholding the precautionary application made by Meta Platforms Ireland Limited, it had suspended the AGCOM regulation on fair compensation.[1]

The Regional Administrative Court had also referred the matter to the Court of Justice of the European Union for a preliminary ruling, and the Council of State, before which AGCOM had brought the matter, could do nothing about the legitimacy of this reference for a preliminary ruling now made by the court of first instance, and on which the European Court of Justice would have to rule, regardless of the appropriate annulment of the precautionary suspension of the AGCOM regulation - which had been ordered by the Regional Administrative Court.

---

* Article for the monography issue on the topic of fair compensation of the Journal 'Diritto ed Economia dei mezzi di comunicazione'.

[1] Regulation on the identification of reference criteria for the determination of fair compensation for the online use of publications of a journalistic nature pursuant to Article *43-bis* of Law No. 633 of 22 April 1941, approved by Resolution No. 3/23/CONS of 19 January 2023. This AGCOM regulation reiterates the Legislative Decree, 12 December 2021, No. 177, Implementation of Directive (EU) 2019/790 of the E uropean Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC (so-called "Copyright Directive").
Lastly, it should be added that, after the Council of State's decision, Meta again appealed to the Regional Administrative Court (TAR), re-proposing again the application for suspension of the aforementioned Regulation, but in this case the same Fourth Section of the Lazio Regional Administrative Court promptly rejected the appeal, complying with the Council of State's decision (Tar Lazio, ord. no. 1929/24, G.R. 4893/24, published on 16 May 2024).

Thus, thanks to the intervention of the Council of State, the trial of the regulation should be able to continue, in the hope that this setback, which certainly constituted an additional obstacle, will help to fuel the necessary attention that the problem deserves.

In particular, the relevant issue is how to balance the different interests that the law, in implementing the directive, considers but does not compose.

From this perspective, the regulation around which this case revolves could be an Italian model, also to be exported, to solve the well-known problem of the difficulty for national regulators to impose rules on digital platforms.

The territoriality limits of state laws, which are incapable of regulating the global space of the internet network,[2] have led, following the suggestions of the doctrine, to experiment with the use of more modern and effective regulatory techniques: 'self-regulation',[3] 'co-regulation'[4] and 'participatory regulation',[5] all based on the principle of subsidiarity under Article 118 of the Constitution.[6]

Since the suspension has been lifted, the pending referral to the EU Court - as things stand - should not prevent the continued development of the desired experimentation of the regulation, which should also be carefully scrutinised by the Court of Justice itself, in order to grasp its potential for solving a problem that is becoming increasingly serious and urgent to solve not only in Europe.

Meta Italia, by opposing the experimentation of the fair compensation system (anything but invasive and at an almost irrelevant cost for the gigantic size and capacity of the platform), has caused harm to all platforms that should, instead, develop their own codes of self-discipline and conduct in a spirit of loyal cooperation and not, instead place themselves in open conflict with States.

---

[2] As long ago authoritatively noted by N Irti, *Norma e luoghi, problemi di geo-diritto*, (2001)

[3] Cf. A Bellelli, *Soft law and co-regulation*, in *Manuale di diritto privato dell'informatica* (edited by R. Bocchini 2023) 51.

[4] Cf. F Bassan, *Digital Platforms and Global Law* (Edward Elgar Publishing, Cheltenham, 2021); U Malvagna, M Rabitti, Filiere produttive e Covid-19: tra rinegoziazione e co-regolazione (2020) (4) Nuovo Dir. Civ., 369 ff.; M Rabitti, Le regole di supervisione nel mercato digitale: considerazioni intorno alla comunicazione Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-activity (2022) (Suppl. n. 3 to n. 1) Riv. Trim. Dir. Econ., 119 ff.

[5] Cf. F Bassan, *Digital Platforms and Blockchains: the Age of Participatory Regulation* (2023) (7-34), European Business Law Review, 1103-1132, which explains what co-regulation is and what the author calls 'participatory regulation'. F Bassan, M Rabitti, Recent evolutions of contracts on the blockchain. From smart legal contracts to 'contracts on chain' (2023) (III) Banking Law, https://rivista.dirittobancario.it/recenti-evoluzioni-dei-contratti-sulla-blockchain-dagli-smart-legal-contracts-ai-contracts-chain). 'Participatory regulation' is a new form of co-regulation, in which the roles of regulators and the market are less defined and can be reversed, with cooperation between market participants, regulators and legislators beginning immediately. In other words, while in the classic co-regulation mechanisms the process begins with the authorities drawing up texts and proposals for rules, which the market then comments on, taking part in consultation procedures; on the other hand, in 'participatory regulation' legislators, regulators and operators work together right from the initial phase of product and service creation, to jointly draw up the minimum requirements deemed suitable to guarantee compliance with continental European *welfare*, which the market must then comply with, according to the so-called 'regulatory circle'.so-called '*regulatory circle'* of rules that originate from the market and return to the market (i.e. first the market tends to align itself with *best practices*, which are transformed into *standards* by national authorities, which then share them in European fora, transforming them into European *standards*, in some cases even into '*technical rules'*, which then in turn return to the market. See also footnotes 4 and 7.

[6] See M Nuzzo, *Il principio di sussidiarietà nel diritto privato* (2014) vol. I, II.

And, above all, platforms should not also stand against those states that (as ours did in this case), far from authoritatively imposing rigid heterodetermined rules, are attempting to favour the use of new sources of discipline[7] (mostly *soft law*) based, precisely, on *co-regulation*, 'participatory regulation' and experimentation (according to the modern model of the regulatory *sandbox*).[8]

That there had not been a 'fair cooperation' approach on the part of the platforms had already become apparent due to the manifest insignificance of the fair compensation offers that (in the brief and unfortunate experiment of the regulation) the platforms had begun to propose to publishers.

Consider, for example, the insignificance of the proposed 'annual' figures (which are maximally degraded for smaller local newspapers).

Some concrete data would be very eloquent in order to grasp what level of (un)willingness to negotiate has been manifested by the platforms in this beginning of the experiment, given that they have only offered very few hundred euros per year to the Italian newspapers,[9] and, therefore. these offers are evidently insufficient to integrate the minimum requirements of good faith in the negotiation.[10]

To have an idea of the social role of publishing companies in guaranteeing pluralism and freedom of information, and therefore also of the extent of the costs incurred, it is sufficient to consider the importance of the "subjective right" of publishers to receive the public contribution to publishing, now pacifically recognised as such in ordinary, administrative and constitutional jurisprudence, and recently reaffirmed by the United Sections of the Supreme Court of Cassation with the sentence Cass. Sez. Unite, 13 May 2022, no. 15370.[11]

This refractoriness to rules (even of *soft law* and self-discipline) and this lack of willingness of digital platforms to dialogue with the social partners of the *platform economy* has serious consequences in terms of social sustainability

---

[7] For an analysis of the "*growing positioning of other regulatory techniques ranging from* Nudging *strategies to* Engagement *mechanisms to the automation of law by technology*", see M Rabitti, *Modelli partecipativi di gestione e prevenzione dei nuovi rischi di impresa tra regolazione e vigilanza*, AA.VV., *Le clausole generali nel diritto dell'economia* (2024) 143.

[8] In Italy, the first rule providing for the "*regulatory sandbox*" was included in Article 36, paragraph *2-bis* of Decree-Law 34/2019 (the so-called "Growth Decree") delegating to the Ministry of Economy and Finance ("MEF") the issuance of one or more decrees to regulate fintech experimentation "*aimed at the pursuit, through new technologies such as artificial intelligence and distributed ledgers, of service and product innovation in the financial, credit, insurance and regulated markets sectors*". Subsequently, on 17 July 2021, the MEF's implementing decree came into force, establishing at it a *Fintech* Committee whose main function is to define the objectives and mediate between industry operators and supervisory authorities, In concrete terms, the Italian sandbox, along the lines of the English model, consists of an environment in which fintech operators engage with the relevant supervisory authorities by experimenting with innovative products and services in the banking, insurance and financial sectors for a limited period of time, against a simplified regulatory regime.

[9] Undoubtedly, the parameters of *fair compensation* (which is a fee based on the revenues that platforms obtain for the exploitation of content created by publishers) cannot be equated with those of the *public contribution to publishing* (which, instead, is only recognised to particular types of publishing companies, and is determined as a partial reimbursement of costs incurred). Structure and function are different, and certainly one cannot claim to charge platforms the cost of public support to publishing. Nonetheless, the extent of the public contribution (where it exists) contributes to demonstrating the insignificance of the fair compensation offers that platforms have seen fit to propose.

[10] Instead, the same minimum requirements of good faith were duly taken into consideration by the same TAR in another ruling that saw Meta Italia losing in favour of AGCM and Siae, to which we will return below (see paragraph 4).

[11] On this point see for all A Parisella, Contributi all'editoria e diritti soggettivi (2023) (3) Diritto ed Economia dei Mezzi di Comunicazione, 55 ff.

and, to some extent, also reputational and *Corporate Social Responsibility* of the '*over the top*' platforms (especially the largest ones, i.e. the so-called VLOPs, Very Large Online Platforms), which increase the risk of inexorably exacerbating the problem of identifying the rules that these platforms should respect, but which states are not able to impose, given the limits of territorial sovereignty.[12]

This evident de facto power leads to the legitimisation of the thesis according to which the most important platforms can be qualified in terms of 'private orders'[13] , so that it is necessary to experiment with new sources of regulation, such as co-regulation or 'participatory *regulation*'.[14]

It seems paradoxical that platforms, in what certainly appears to be a selfish and one-sided view, accuse states of violating freedom of economic initiative by imposing rules that would be contrary to the free flow of information. No account is taken of the fact that, on the other hand, the issue of freedom and pluralism of information is a delicate one and cannot be left to mere market logic. The protection of freedom of information is by no means a limitation, but a virtue, so public support and intervention is necessary to guarantee Article 21 of the Constitution. [15]

The decision of the Regional Administrative Court did not seem to have adequately assessed the aforementioned problems and ended up endorsing the '*power of the platforms*', preventing the State from not only 'dictating' but also just 'competing' in regulating the information market.

Instead, it is necessary to protect and balance the rights of publishers and users of information, which remain at risk of being undermined by the uncontrolled and uncontrollable dictatorship of the platforms themselves that could not be opposed by any rules, not even by 'sharing' them, contrary to the dialogic culture to which the directive expressly refers.

Above all, attention must be paid to the *public interest*, i.e. the benefits that the fair compensation discipline may bring to the public of network users using platforms, who may continue to enjoy, through the network, the publishers' copyright-protected content, free of charge (leaving aside here the well-known problem of the 'sharing' of their personal data that platforms acquire)[16] .

The legitimacy and appropriateness of the regulation on fair compensation should also be assessed in view of AGCOM's role of supervision, control and regulation of the market for the *online* dissemination of publishers' information content. From this point of view, AGCOM, in the free communications market, which, however, in compliance with the law, can and

---

[12] On which see again N Irti, *Norma e luoghi. Problems of geo-law*, cit

[13] This refers to the thesis of F Bassan, op. cit. (see footnotes 4, 5 and 7).

[14] See footnote 5.

[15] Cf. again A Parisella, op.cit. Moreover, the directive itself emphasises the importance of this profile, as can already be deduced from recital 54, which states that: "*A free and pluralist press is essential to ensure quality journalism and citizens' access to information and makes a fundamental contribution to public debate and the proper functioning of a democratic society*".
With particular reference to the importance of the discipline of fair compensation introduced by the European *Copyright* Directive in the aim of supporting pluralism of information, see A Papa, *La tutela del pluralismo informativo in Rete. The role and perspectives of European Directive 2019/790*, AA. VV., *Il diritto d'autore nell'era digitale*, (edited by A. Papa 2023), 13 ff.

[16] On this point, see for all C Irti, *Consenso "negoziato" e circolazione dei dati personali* (2021) V Ricciuto, *L'equivoco della* privacy. *Persona* vs *personal data* (2022).

must be regulated by the authority appointed for this purpose in our legal system[17] , is obliged to balance not only the (private) interests of platforms and publishers, but also the general interest of information users.

The problem is resurfacing with an even more serious and important target than the regulation on fair compensation: the platforms are now aiming to challenge even the R.O.C. (Register of Communication Operators), kept by AGCOM, which is a more modern and evolved system compared to the old registration of newspapers with the Courts, which was historically inspired by the now outdated logic of combating the clandestine press. The platforms thus show that they refuse even to subject themselves to those minimal forms of taxation and control necessary to manage the public register of 'communication operators', which are very useful for guaranteeing the quality and reliability of information and protecting pluralism.

Amazon has already filed this appeal, as it had already announced in the consultation.[18] Hence, this other (small) stake - the R.O.C., with which one could attempt some kind of regulation of the communication market, in which the increasingly powerful digital platforms, with increasingly weakened states, have made inroads, is also at risk.

2. The perplexities raised by the Lazio Regional Administrative Court's (TAR) judgment No. 18790 of 12 December 2023 (Meta v. AGCOM), duly reformed by the Council of State (Order No. 894 of 11 March 2024): the need to balance digital services with fundamental rights.

The approach that the TAR had taken in this matter of the regulation on fair compensation favoured the aggressive dominance of platforms, which, among other things, are currently de-indexing newspaper sites and tend to abandon the construction of news, entrusting it - instead - to the uncontrolled composition by so-called 'generative' artificial intelligence systems.[19]

Here is then, as one of the inevitable consequences of feeding a conflict between antithetical positions, with no attempt at mediation, the result of the glorious New *York Times* newspaper suing OpenAI, Microsoft (and others), forbidding *ChatGPT* from using its content.[20]

This is not the place to dwell on the issue that lies at the heart of a debate, quite intense in the United States (and elsewhere), which focuses on the analysis of the activity of processing intellectual works through the use of

[17] Against claims of naturalness, in the sense that the market consists of the 'statute of rules' created by the legislator (even when he chooses not to intervene) and is therefore always *locus artificialis*, cf. N Irti, *L'ordine giuridico del mercato* (1998).

[18] See Annex 1 to Resolution No 270/23/CONS containing the Summary of Comments to the Public Consultation on the Proposal to Amend the Regulation for the Organisation and Maintenance of the Register of Communication Operators, in https://www.agcom.it/documents/10179/32496245/Allegato+28-11-2023/1e3b1174-cde9-4054-83b6-90ab7f99b5fc?version=1.0.

[19] On the economic consequences of an uncontrolled development of such systems see S Da Empoli, *L'economia di ChatGPT. Tra false fears and real risks* (2023) 53 ff.

[20] Application No. 1:23-cv-11195 of 27 December 2023 brought before the United States District Court for the Southern District of New York, courthousenews.com. See at also footnote 38.

artificial intelligence,[21] asking whether or not it is creative, and consequently whether or not it is subject to copyright protection. Indeed, regardless of how the question is resolved, it makes it possible to reiterate with certainty that the various ways of using newspaper content (whether or not they are susceptible to copyright protection) evidently represent an unjustified enrichment of digital platforms to the detriment of newspapers themselves, which as a result of this *trend* will eventually disappear, also seriously undermining the pluralism and independence of information.

It is recent news that Meta has shut down its '*News*' section in the United Kingdom, Germany and France (i.e. the European countries where the service had been activated, among which Italy has never been included), and then also in Canada and Australia, thereby - in effect - refusing to carry newspaper content. Given that these very countries (as will be seen)[22] have adopted or are attempting to adopt legislation on the subject, aimed at considering *online* platforms as any other content publisher and consequently subjecting them to taxation or other rules, it can be seen that the policy of these '*over the top*' platforms, not only in Italy, runs the risk of being in open conflict with any rule.[23] In essence, in order not to agree to submit to rules (albeit shared ones), Meta decided to reverse its policy of disseminating information content, ousting it from its platform. But by doing so, the conflict with states is exacerbated and the users of content themselves are harmed.

The problem (as has already happened in Italy for music)[24] could backfire on the platforms themselves, should the platform in question (in this case Facebook) be deemed to have assumed such importance as a vehicle for the

---

[21] Cf. J C Ginsburg, Fair use in the United States: transformed, deformed, reformed? (March 2020) Singapore Journal of Legal Studies, 265-294, also available *online* at https://law1.nus.edu.sg/sjls/articles/SJLS-Mar-20-265.pdf; J C Ginsburg, L A Budiardjo, Authors and Machines, in Berkeley Technology Law Journal (2019) (2-34), 358 ff, also available online: https://lawcat.berkeley.edu/nanna/record/1136665/files/01_Ginsburg_Web%5B1%5D.pdf?withWatermark=0&withMetadata=0&version=1&registerDownload=1

[22] See para. 3.

[23] The terms and risks of the problem for the survival of newspapers are highlighted, with stark clarity, by V Ghionni, Facebook e l'equo compenso: la discussione sul nulla, in https://www.editoria.tv/facebook-e-equo-compenso-la-discussione-sul-nulla/, 2 March 2024, who observes that: "*The dispute between Meta and the Communications Guarantee Authority over the application of the law on fair compensation is being followed with great attention by newspapers. Fieg associates itself with the Authority's appeal, applauds, smiles and thanks. Meta believes that it should not be subjected to Italian regulations and the Regional Administrative Tribunal agrees with it. It is discussed, it is debated, it is enough to think that almost four years have passed since the EU directive that provided for fair compensation for publishers to the Authority's resolution. In that time, newspaper publishers have lost millions of copies and the over the top have gained billions of euros, refined their algorithms, and further strengthened their centrality in the market and their ability to influence public opinion. The rationale of fair compensation is to rebalance the market, to take a little from those who publish content to give something to those who produce it. In 2019, when the EU resolution was issued, artificial intelligence was still science fiction, today it is reality. There was no war in Ukraine that further polarised the debate, content was still a value. But while the courts decide, publishers applaud and solons debate, Meta continues to grind out profits, publishers lose copies and turnover. The only ones who stay quiet are the solons because there is always a coffee break or a light lunch between a symposium and a seminar. And someone applauds. Then comes news from overseas that causes a stir, Meta closes its news sections in Australia and the United States. Too bad it had already done so a few months ago in France, the United Kingdom and Germany, they no longer need the content of others, artificial intelligence has meanwhile become a reality, and so why throw money at newspapers when the algorithm obeys its master better than the most paludate reporter. In a few months the Council of State will decide in the Meta-AgCom case, more time will have passed, the newspapers will have continued to lose copies and turnover, and Meta will have gained and increased its ability to influence public opinion. If it loses in the courts, it will also deactivate the news section in Italy. And it will be an argument for the Solons*."

[24] See para. 4.

online circulation of information content,[25] so that it is not fungible in the absence of other equivalent instruments and is therefore obliged to convey all content, without being able to exclude it, almost like a *monopolist of a public digital service*.

These quick hints already appear to be decisive in order to make us meditate on the importance of experimenting with the discipline of fair compensation, which could contribute to achieving (not only in Italy) a 'shared' balance, between the rights of platforms, publishers and - above all - users of information.

Isn't it better to agree on a meeting point between copyright and the free dissemination of content on the net, as the regulation of fair compensation to publishers aims to achieve?

The logic of confrontation between parties operating in a context characterised by complexity does not seem to lead far, and instead seems to aggravate problems that are already difficult to solve.

It is necessary for all social actors - authorities, judiciary, doctrine - to be culturally prepared to understand and deal with the new technologies and new sources of law that inevitably have to be employed.

Certainly the platforms, in light of the context in which they operate, are not a 'weak party'. It seems somewhat anomalous that the TAR has stated (even several times) that they would even be in a situation of 'subjection'.[26]

One of the most perplexing points of the ruling can be found in the qualification of the co-regulation mechanism as '*compulsory arbitration*'. After such a statement, the following pages instead speak of "*arbitrage*" (cf. p. 26f), thus increasing the confusion of the qualifications of the case by referring to Art. 1349 of the Civil Code.[27] The Regional Administrative Court had stated (see p. 6) that "*Article 43-bis L.a. (and, therefore, the Resolution and the Regulations implementing it) introduced a right to remuneration (fair compensation) that can be interpreted as (or, in any event, substantiated by the de facto introduction of) an 'obligation to negotiate', which significantly restricts the contractual freedom of economic operators and to which an 'obligation to pay' attaches*".

Furthermore, the Court had stated (see p. 7 s.) that such new regulatory interventions would be '*contrary to the freedom of enterprise*' because they would imply: 1) a determination of tariffs and a provision for a '*compulsory arbitration procedure*' (which would reintroduce, de facto, a form of authoritative determination of the prices of products freely traded on the

[25] It is no coincidence that in the statement with which Meta itself announces the service's discontinuation, it takes care to justify its decision by citing the lack of success of news on the social network: "People do not come to Facebook to read news and political content but to connect with others and discover new opportunities, passions and interests. News represents less than 3% of what is seen on Facebook feeds, a small part of a much larger experience for the vast majority of users". The social giant is also keen to point out that the changes affecting *Facebook News* will have no impact on Meta's products and services in these countries, and people will still be able to view links to news articles on Facebook. News publishers will continue to have access to their Facebook *accounts* and pages, where they can post links to their stories and encourage people to visit their websites, in the same way any other individual or organisation can.
In addition, newspapers will also be able to leverage products such *as Reels and* Meta's advertising system to reach a wider audience and direct people to their websites.

[26] See pages 23 and 27 of the cited judgment (although not numbered).

[27] On this point - because of the clear and well-known distinction between *arbitrators*, who decide legal disputes, and arbitrators, who determine the economic content of a contract - the reference to F Carnelutti, Arbitri e arbitratori (1924), in Riv. dir. proc., 6 ff.

market); 2) a '*significant limitation of contractual freedom*'; 3) an obligation not to restrict visibility in the search results during negotiations (in violation of the EUCD and the enabling act, which do not provide for any such rule); 4) a "*role entrusted to Agcom*" (to which one of the parties could turn during negotiations to activate a procedure for determining remuneration) 5) "*disproportionate and discriminatory criteria to be taken into account to determine the fair remuneration*" (such as the number of journalists employed and the importance of the publisher, criteria also contested in an AGCM opinion); 6) "*obligations to make data available*" (to be fulfilled by the ISSPs, at the request of the party concerned or of AGCOM), with the latter's sanctioning power being accepted 7) '*inspection powers*' granted to AGCOM (to acquire the parameters necessary for determining fair compensation); 8) '*obligations to make data available that have no legal basis, are disproportionate and contrary to the EUCD*'.

Even violations of constitutional principles, such as the freedom of economic initiative, the principles of proportionality and reasonableness, the principle of equality and non-discrimination (for the '*unreasonable*' benefit granted only to publishers), would occur, according to the TAR.

But this decision completely overlooked the source of 'co-regulation' and 'regulated autonomy', which is the basis of modern 'private regulatory law'.[28]

Above all, the focus on the *audience* that benefits from the content disseminated by the platforms was missing. This is a market interest that the state must protect and favour.

The digital platform, on the other hand, is not a weak party to be protected in a 'private negotiation'. And the authority is by no means a '*strong contractor*' acting in its own interest, but rather a public entity that - precisely in the public interest - must be able to exercise its powers of control and even sanction.

This is not to deny that the regulation on fair compensation, launched by AGCOM on 19 January 2023, on the basis of Legislative Decree 177/21 implementing Directive (EU) 2019/790,[29] may be susceptible to improvement, or to revocation in doubt that there is reason to raise problems of compatibility of the transposing regulation with the European directive.

However, the Copyright directive itself (in particular art. 15 "*Protection of journalistic publications in case of online use*") and its implementation through the Italian regulation of fair compensation under discussion here, must necessarily be interpreted in the light of all the fundamental freedoms protected by the Charter of Fundamental Rights of the European Union (CFREU), the ECHR and also by our Constitution (and first of all the freedom of information under art. 11 CFREU, 10 ECHR and 21 Constitution, which is also in the purpose of the directive itself that aims to protect copyright);[30] so that one cannot neglect to consider the balancing of all the interests at stake, limiting

[28] See A Zoppini, *Il diritto privato e i suoi confini* (2020); M Angelone and M Zarro (eds.), *Diritto civile della regolazione: conformazione degli atti di autonomia e disciplina dei mercati* (2022).

[29] See footnote 1.

[30] The relevance of these principles is also found in Article 2 TEU which, in recalling the founding values of the rule of law, also refers to pluralism. On the essentiality of press freedom for democracy, see, from the perspective of European regulation, R Mastroianni, *Freedom and pluralism of the media: an European value waiting to be discovered?* (2022) (1), Medialaws, 100 ff. Going back to the origins, we cannot fail to recall the famous pages of J. Milton, *Areopagitica, Discorso per la libertà della stampa*, Translation and preface by S. Breglia (1933) (reprinted in Diritto ed Economia dei Mezzi di Comunicazione, 2021,2).

oneself instead to an isolated focus only on certain profiles of market rules and freedom of economic initiative.

Moreover, today the balancing of the rules for the provision of digital services with fundamental rights is expressly imposed by Article 14 of the *Digital Services Act* (with the aim of improving the moderation of content on social media platforms to address concerns about illegal content),[31] and the European Court of Justice will certainly have to take this into account, as well as (in addition to the aforementioned DSA) also the *Audiovisual Media Services Directive (AVMSD*) , the [32]Digital Market Act (DMA)[33] and the very recent *European Media Freedom Act (EMFA)*, approved by the European Parliament on 13 March 2024, which aims to protect the European media from political or economic interference, in order to protect precisely the right to information, with particular attention to the pitfalls generated by digitalisation.[34]

The speed of the digital revolution and its impact on the world of news and publishing demands an immediate solution to make the advent of *online* dissemination via platforms compatible with the content produced by newspapers. AGCOM was urged to adopt it promptly, especially by publishers who demanded a quick solution to the problem[35] (and the regulation on fair compensation also met with consensus and constructive encouragement). [36]

---

[31] Art. 14 of the DSA (Digital Services Regulations, approved as EU Regulation 2022/2065, aiming to "*contribute to the proper functioning of the internal market for intermediary services by establishing harmonised rules for a safe, predictable and reliable online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected*") takes a first important step towards so-called *digital constitutionalism*, i.e. the adaptation of constitutional values to the peculiarities of the digital environment. In fact, the DSA introduces an obligation to consider in the implementation and application of the terms of service also the fundamental rights of citizens ("incorporate fundamental rights into the TOS"), in particular freedom of expression and media pluralism. Furthermore, it is expressly stipulated that platforms must act diligently and proportionately, and not arbitrarily or discriminatorily.

[32] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018, which aims to ensure the proper finalization of the digital single market in the EU for audiovisual media services, while contributing to the promotion of cultural diversity and providing an adequate level of consumer and minor protection.

[33] Regulation (EU) 2022/1925, aimed at ensuring that digital markets in which *gatekeepers* (access controllers) are present are fair and contestable throughout the EU.

[34] With this piece of legislation - in which there is a heightened awareness of the need to implement cooperation between the competent national authorities in order to combat regulatory fragmentation and therefore to resort to co-regulation, based on dialogue with the most relevant platforms (which, pursuant to Art. 17, must make a declaration in which, among other things, they certify that they are independent and that they operate in accordance with co-regulatory and self-regulatory mechanisms) - among other novelties, a mechanism is introduced that aims to prevent *VLOPs* (*Very Large Online* Platforms), i.e. the largest digital platforms, from arbitrarily restricting or removing independent media content. In fact, large *online* platforms are asked to distinguish independent media from non-independent sources and give them 24 hours to respond before removing content. Once this time period has elapsed, the platforms will be able to proceed with the removal and the media will be able to appeal by turning to an out-of-court dispute resolution body. The media will also be able to seek the opinion of the European committee for media services, (composed of national regulators) established by the new law (see Art. 8). The direction, therefore, is to prevent platforms from excluding or 'cutting off' from their digital channels newspaper content, which, on the other hand, must necessarily be disseminated through them.

[35] See article in 'Repubblica' of 15.12.2022, *The transposition of the EU directive. Publishers: the Authority approves the copyright regulation. Criteria for the remuneration of those who produce content shared on the web have been awaited for 10 months*.

[36] See, e.g., M L Bixio, V Falce, Brevi note sul principio di "fair remuneration" e "fair contract" nella Direttiva Copyright, (2020) (4-5) Rivista di diritto industriale, 261-288; V Falce G Ghidini, Copyright digitale, il decreto non va annacquato, Corriere della sera, 3 August 2021, who, with reference to the Italian transposition of the Directive, observe that: "*Commendably, the Italian draft of the decree envisages, in order to ensure the effectiveness of the rule, a negotiated procedure aimed at promoting a "good faith" agreement between*

The dissenting voices had also been joined by the AGCM, which had expressed a negative opinion (referred to several times in the TAR ruling), finding profiles of violation of the principles of freedom of economic initiative and free competition, which would be jeopardised by these rules requiring platforms to pay fair compensation to publishers.

Even from within AGCOM itself there was the voice of a commissioner who had not failed to voice her dissent with regard to the resolution of the college of which she is a member, again believing that an 'obligation to buy' would be imposed on platforms.[37]

The Council of State put things in order by clarifying that the AGCOM Regulation does not introduce any obligation to negotiate, but rather "*provides, in fact, for a mechanism to reach an agreement, but the right to bring an action before the competent court remains unaffected*" (see p. 16).

But the point is that it would not be a question here of the introduction of a simple obligation to negotiate imposed on private actors in the free market, but of market protection aimed at protecting publishers and the right to information by seeking new criteria of balance and equilibrium in the general interest.

It should be borne in mind that the regulation of fair compensation aims at balancing the interests of the publishers producing the content, which is encompassed by the platforms that use it by disseminating it (even if modified and innovated) to the audience of users.

Not only are platforms not allowed to enrich themselves by unduly exploiting content created by other authors, but they must also be obliged to acquire it - by paying fair compensation to the publishers who generated it - and then disseminate it for the benefit of users through their digital channels, which have now become essential and infungible in the market.

The protection of the right to information therefore requires, on the one hand, that platforms purchase, but also, on the other hand, that authors allow the dissemination of information content, so that even publishers, being remunerated by fair compensation, cannot prevent their content from being used for the benefit of the public that uses the services of the platforms.

This is why fair compensation also proves to be an advantage for platforms and the user public, who are not deprived of knowledge that must be made 'common' for the completeness of the knowledge and data circulation on which creative artificial intelligence systems are based by the platforms themselves.[38]

---

publishers and platforms - like the one already stipulated between Google and Cairo Editore. In the event of a stalemate, each of the parties will be able to turn to AgCom to set the price. A sort of regulatory dialogue, in short, in which Agcom, in addition to the role of arbitrator, has the task of defining certain and fair criteria for negotiation (among the main ones, we would say: the different circulation of the newspapers involved and the different 'informational autonomy' of the 'appropriate' pieces). The draft that will go to the Council of Ministers is solid and as such deserves to come out without contamination and watering down"; Cf. also issue no. 1/23 of the journal "Diritto ed Economia dei mezzi di comunicazione", entirely dedicated to legislative decree no. 177 of 8 November 2021 on fair compensation for publishing companies, which opens with the editorial by A Di Amato, Riuscirà l'equo compenso a contrastare il declino dei giornali? See, among other comments in the same issue, V Ghionni, Gli impatti del decreto legislativo sulle imprese editoriali, 57 ff.

[37] Thus E Giomi, Meta's appeal to the Tar highlights the fragility of the Agcom regulation, https://www.huffingtonpost.it/blog/2024/02/15/news/il_ricorso_di_meta_al_tar_mette_in_luce_alcune_fragilita_del_regolamento_agcom-15142916/.

[38] The functioning of the fair compensation discipline, therefore, could prevent the risk of disputes such as the one currently underway between the New York Times and Open AI - ChatGPT (see footnote 20), which,

Fair compensation allows platforms the benefit of '*ingesting*' even proprietary data.

The completeness of data is essential for knowledge[39] and thus for the functioning of AI systems that work by processing them.

Therefore, there is a need to balance the *opt-out* mechanism (i.e., the ability of copyrights holders to exclude the use of their own data)[40], with the need of platforms to acquire them in the public interest (thus not for their own commercial purposes): and the fair compensation regulations aim to achieve this goal.

That is why it is also worthwhile for platforms to seek the right balance to balance the interests of all. Otherwise, a conflict is exacerbated, not only with the publishers (who risk becoming extinct, thus undermining the freedom and

---

moreover, is widening as eight other U.S. newspapers owned by the hedge fund Alden Global Capital (including the New York Daily News and the Chicago Tribune) have also sued Open AI and Microsoft for the same reason, believing that the platforms must "obtain publishers' consent to use their content and pay fair value for that use." This is despite the fact that in other cases Open AI itself is showing that it has begun to enter into agreements with large publishing groups (including Associated Press, Shitterstock, and in Europe the German group Axel Springer, the Spanish group Prisa-Promotora de Informaciones, and the leading French newspaper Le Monde).

The result to be avoided is a conflict in which any of the parties would lose: either the producer of the content, who would be deprived of any compensation, or the platform, which could not use it. This hypothesis has, moreover, already occurred, for example, in the case that occurred in the United States with the platform (which was a mere *start-up*) that managed a "predictive" *Ross intelligence AI* system, which closed in the face of the threat of litigation by the owner of the patent on the legal database used for the operation of the system, which - therefore - inexorably ceased to exist (see https://www.law.com/therecorder/2023/12/15/thomson-reuters-v-ross-intelligence-ai-copyright-law-and-fair-use-on-trial/).

The problem is well understood by analysts advising the US government, as we read in G Pellicano, Is there a transatlantic way to AI? Pellicano's proposal, in Formiche.net (https://formiche.net/2024/03/intelligenza-artificiale-pellicano/) who notes that "*Further repercussions of the use of artificial intelligence concern the respect of copyrighted data and the definition of the concept of fair use, i.e. the limited and lawful use of copyrighted materials. The recent initiative of the* New York Times *to sue OpenAI for the unlawful use of its archives for AI training could lead to the jurisprudential or transactional establishment of new limits on the use of copyrighted texts. Here again, the solution may come from a decision imposed by public authority or from an agreement between the parties that may open the door to shared self-regulation between companies with opposing interests. An effective analysis of what is at stake for publishers and artificial intelligence programmers was published in October by Colombia Journalism Review: An AI engine scans a book. Is that copyright infringement or fair use?*".

After all, a culture of aversion against overly restrictive forms of protection for creative works in the age of digitization, which demands free sharing of data, is gaining in popularity and awareness. Among the most active exponents of this movement of thought, see, for example, C Doctorow, who in his own biography (published on his website "Creative Commons" since 2006), states: "*I believe that we live in an era where anything that can be expressed as bits will be. I believe that bits exist to be copied. Therefore, I believe that any business-model that depends on your bits not being copied is just dumb, and that lawmakers who try to prop these up are like governments that sink fortunes into protecting people who insist on living on the sides of active volcanoes*" (see https://wiki.creativecommons.org/wiki/Case_Studies/Cory_Doctorow).

[39] E Ostrom, C Hess, *Knowledge as a Common Good*, (2009). See also P Springhetti, *L'informazione è un bene comune. Riflessioni sulla mediaetica* (Ucsi 2013), P Aigrain, *Causa comune. L'informazione tra bene comune e proprietà* (Stampa alternativa 2007). With specific reference to the problems of free use of data excluded by authors in artificial intelligence systems, see G M Ziaja, *The text and data mining opt-out in Article 4(3) CDSMD: Adequate veto right for rightholders or a suffocating blanket for European artificial intelligence innovations?*, (2024) (19-5) Journal of Intellectual Property Law & Practice, 453-459, also available online at https://doi.org/10.1093/jiplp/jpae025.

[40] The opt-out principle is adopted in the European AI Act (approved on March 13, 2024) and would also be shared in a new Italian draft of bill on Artificial Intelligence provisions and delegation to the Italian Government (approved by the Italian Government on April 23, 2024) which has provisions also on copyright (in this way the platforms do not have to indicate the source, but the media have the duty to "mark up" content generated or modified by AI, to make it recognizable to users).

pluralism of information), but also with the user public and thus with the states, with whom the platforms should not refuse dialogue.

And in the long run, conflict does not benefit anyone. Not even the platforms.

Limiting ourselves to recalling the use of terminology, which, however, may be destined to take on different specific meanings in the various contexts, it suffices to recall, in general terms, that the "*obligation to negotiate*" has now also entered into the public contracts code (see Article 9 of Legislative Decree No. 36/2023, which provides for the principle of preservation of the contractual balance, from which derives - precisely - the obligation to contract and the implementation in public contracts of renegotiation clauses).

Even the very notion of "*fair compensation*", not unknown in the copyright legislation[41] and variously used in our legal system (see Article 1526 of the Civil Code on fair compensation due to the seller in the event of non-performance of the buyer in the sale by instalments and Law no. 49 of 21 April 2023 on fair compensation for professional services), would deserve further consideration, also with regard to its judicial determination, which could integrate something quite different from an obligation to "buy" or to impose a "price".

On closer inspection, here fair compensation (the *quantum of* which is not a direct consideration referring only to economic utility) goes beyond a merely negotiated logic, but constitutes a *compensatory measure necessary for the proper functioning of the market*, the determination of which, instead of being immediately and authoritatively imposed, one would like to try and refer, hopefully, to a sharing between the protagonists, under the aegis of the competent authority. The point is not so much to negotiate a fee between the parties on the basis of market parameters[42] , but to find a balancing criterion that guarantees the market by protecting all players, almost like a 'tax' imposed on the party that makes the biggest profit.[43]

---

[41] For an analysis of the various precedents in Italian law, see L Attolico, *The equitable remuneration of authors and artists for the exploitation of their works and performances in the digital market: novelties and perspectives in the light of the new* copyright *directive*, Il diritto d'autore nell'era digitale, cit. 87 ff. In particular, in Art. 70 ff. of the Copyright Law, it is established that copyrighted data can be freely used-as long as it is not for profit but for educational or scientific use or for criticism or discussion (without constituting competition to the economic use of the work)-referring to regulations that establish "*the manner for determining fair compensation*" (see Art. 70, paragraph 2, Law 633/1941).

[42] The parameter for determining fair compensation does not work according to a normal economic criterion of the exchange value that the information content generated by the author would have, since this value is created (or amplified) by the same platform that employs it on the network (on this "paradox of value" see C Mazzoni, Creation and Distribution of Value in the Non-Fungible Token (NFT) Market, 2024) (1) Diritto ed Economia dei Mezzi di Comunicazione 77 ff.

[43] On closer inspection, such a law, although it has remained a dead letter (and therefore its scope should be assessed, also by coordinating it with the rules on fair compensation under consideration here), already exists: see Law No. 198 of 26 October 2016, which established the "*Fondo unico per il pluralismo e l'innovazione digitale dell'informazione e dell'editoria*" (*Single Fund for pluralism and digital innovation in information and publishing), which,* in Article 1, paragraph 2, expressly states that: "*2. The Fund shall include: a) state resources allocated to the various forms of support for daily and periodical publishing, including digital publishing, including the available resources of the Extraordinary Fund for publishing support interventions, as per Article 1, paragraph 261, of Law No. 147 of 27 December 2013; b) state resources allocated to radio and television broadcasting in the local area, entered in the estimates of the Ministry of Economic Development pursuant to Article 1, paragraph 162, of Law No. 208 of 28 December 2015,. 208; c) a share, up to a maximum amount of €100 million for the year 2016 and €125 million for each of the years 2017 and 2018, of any increased revenue paid by way of television subscription fees, referred to in Article 1, paragraph 160, first sentence, letter b), of Law No. 208 of 28 December 2015, as replaced by Article 10, paragraph 1, of this Law; (d) the sums deriving from the annual proceeds of a solidarity contribution equal to 0.1 per cent of the total income of the following*

In short, the direction that the Italian legislature has taken to transpose the directive, although susceptible to being refined and perfected, appears useful for testing the new regulatory sources of *co-regulation* and the role of independent authorities in establishing and cultivating the necessary dialogue with the *over-the-top* platforms, in order to share rules suitable for balancing opposing interests and guaranteeing the proper functioning of the market, taking into account not only the economic aspect, but also social utility profiles.

3. The fines imposed on Google by the French antitrust authority.

Certainly, it would be worth investigating how the problem has been dealt with in other countries, particularly at the European level, to see how other states have implemented the directive (well or badly).

It is worth mentioning, if only for illustrative purposes, that in Canada there is a bill[44] , as well as in California[45], and also in Australia there is already a law[46] with the aim of protecting newspaper content and thus obliging digital platforms to compensate publishers fairly for reproducing news (although, as mentioned, it is precisely in these countries that are attempting to legislate on this point, that Meta recently closed its '*News'* section).

But, coming to Europe, it is useful to look at what has happened in France, where - unlike the 'self-critical' approach with which the Lazio Regional Administrative Court had suspended the national discipline by submitting it to the European Court of Justice - not only has there been no referral to the EU Court, but on the French national law (law 2019-775 of 24 July 2019 aimed at

---

persons liable to the tax referred to in Article 73 of the Consolidated Law on Income Tax, referred to in Presidential Decree No. 917 of 22 December 1986 917: 1) concessionaires of advertising sales in the daily newspapers and periodicals and in the radio, television and digital media; 2) companies operating in the information and communication sector that carry out direct advertising sales, in this case calculating the total income with regard to the part proportionally corresponding, with respect to the amount of total revenues, to the specific amount of revenues deriving from such activity 3) other entities that engage in the activity of intermediation in the advertising market through the search and purchase, on behalf of third parties, of space on the media and communication media, with reference to all types of transmission platforms, including the Internet".

[44] First Session, Forty-fourth Parliament, 70-71 Elizabeth II, 2021-2022, House of Commons of Canada Chambre, Bill C-18, An Act respecting online communications platforms that make news content available to persons in Canada, First reading April 5, 2022. This law is referred to by many of the critics of the Italian legislation, who consider that our legislature seems to have been inspired by this 'anomalous' discipline.

[45] California Journalism Preservation Act (CJPA), Assembly Bill no. 886, February, 14, 2023, amended in Senate July, 3, 2023.

[46] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021, No. 21, 2021, An Act to amend the Competition and Consumer Act 2010 in relation to digital platforms, and for related purposes.

Pursuant to this 'News Media Contract Code', launched just three years ago, Facebook and Google had signed a number of agreements with several publishers (including national radio-TV station Abc, Guardian Australia, News Corp Australia, Seven West Media and Nine Entertainment, parent company of the Sydney Morning Herald and The Age newspapers in Melbourne), which the platforms have now stated that they do not intend to renew, let alone renegotiate.

The clash between Meta and the Australian government is taking on tones of serious opposition, as reflected in the statements made by Prime Minister Anthony Albanese, who expressed his strong disappointment at Meta's decision to close the News section, describing it as '*unsustainable*', announcing measures against the platform and declaring that: "*It is dishonest that a company can profit from others' investments, and not just capital investments, but from the work of journalists. It is a breach of its commitment to the sustainability of the Australian news media*' (source ANSA, 4 March 2024).

creating a proximity right for the benefit of press agencies and publishers) the antitrust authority has already intervened with two consecutive pronouncements (2020 and 2021)[47] in order to sanction Google for abuse of a dominant position.

The precautionary and sanctioning measures adopted by the French antitrust authority concern the way in which Google implements the aforementioned Law 2019-775, which transposes into French law Article 15 of Directive No 2019/790 of 17 April 2019 on copyright and related rights in the digital single market, and is precisely aimed at creating the conditions for a balanced negotiation between publishers, news agencies and *online* public communication services, in order to redefine the sharing of value between these actors.

However, in order to comply with the law, Google had unilaterally decided that it would no longer display extracts of articles, photographs and videos of its various services unless publishers granted permission to do so free of charge.

In the interim measures decision, the Authority therefore considered that the practices in question could constitute an abuse of a dominant position.[48]

Therefore, the Commission issued seven injunctions in the interim measures decision in order to redress the balance of power between the various press operators and digital platforms and to establish a mandatory negotiating framework adapted to the circumstances of the case. The injunctions imposed on Google - among others - the obligations to enter into good faith negotiations with publishers and news agencies that so wish (for a period of three months from the date of the publisher's or news agency's request); to disclose the information necessary for a transparent assessment of the remuneration provided for in Article L. 218-4 of the Intellectual Property Code.

4. The judgment TAR Lazio 30 October 2023, no. 16069 (Meta v. AGCM and SIAE).

Even without going abroad, it is worth recalling that the same TAR of Lazio had ruled in the opposite way, and in our opinion much more convincingly for the protection of the digital market, just a couple of months earlier, in the case pitting Meta itself against the AGCM and the SIAE - Società italiana degli autori ed editori (Italian Society of Authors and Publishers). [49]

In the earlier case, the Regional Administrative Court dismissed the appeal brought by Meta to request the annulment of the decision by which the AGCM had ordered it to '*immediately resume negotiations - with Siae - maintaining a conduct inspired by the canons of good faith and fairness, and providing all the information necessary to re-establish a balance in the entire commercial*

[47] The first: Autorité de la concurrence, Décision n° 20-MC-01 du 9 avril 2020, relative à des demandes de mesures conservatoires présentées par le Syndicat des éditeurs de la presse magazine, l'Alliance de la presse d'information générale e.a. et l'Agence France-Presse; la second Autorité de la concurrence, Décision n° 21-D-17 du 12 juillet 2021, relative au respect des injonctions prononcées à l'encontre de Google dans la décision n° 20-MC-01 du 9 avril 2020.

[48] See footnote 50.

[49] TAR Lazio, 30.10.2023, no. 16069/2023 Reg.Prov.Coll., no. 08974/2023 Reg.Ric., no. 08975/2023 Reg.Ric.

relationship and to promptly restore, in full, the availability of music content protected by Siae on Meta's property for the entire period necessary to conclude the negotiations'.

In this case, which had seen the audience of Meta's *social network* users (i.e. *Facebook*) deprived of music content due to Meta's failure to reach an agreement with the SIAE for the fair compensation of the copyright due for the reproduction of the tracks, the Regional Administrative Court took into account the plurality of the underlying interests: in fact, it paid significant attention to the overall picture, which allowed it to take into account the fact that the *social network* of the dominant platform in the new digital market[50] is a space in which the rights of the authors of the content and the users must necessarily be guaranteed, in the public interest.

Hence, the platform was not allowed to selfishly evade the negotiation and thus exclude copyright-protected music content, which it had, therefore, to acquire necessarily by concluding the negotiation.

Here the Regional Administrative Court chose to protect the position not only of the SIAE but also of the AGCM: this is in contrast to what happened to the AGCOM in the other decision under examination here, in which the Regional Administrative Court - conversely - deemed the fair compensation mechanism to be contrary to free competition (moreover, citing in support an opinion in conformity with that of the AGCM itself).

On pg.11 of this judgment - taking well into account the "*overwhelming power of platforms*" (p. 13) and their "*infungible*" role - for authors and the public of users - we read that "*9.9. In the face of these numbers, any impediment to access the platform constitutes a very serious harm for the artists: on the other hand, as effectively represented by SIAE's defence (which cites specialist literature for this purpose), the "discovery" of the musical content tends to take place on social networks, constituting the premise of the subsequent "fruition", either on the dedicated music platforms, or through traditional channels. The fundamental role of the recurring society's platforms in the dissemination of music content is therefore apparent. 9.10. Moreover, it should be noted that the possibility that the products protected by SIAE may be digitally enjoyed in another way does not constitute a satisfactory alternative, given that the closure of Meta's digital channels does not appear to be surrogate by other means: to put it simply, the circumstance that Facebook or Instagram have competitors in the social network market (in particular, Tik Tok) does not automatically imply that the service offered by the latter company can be considered a satisfactory alternative. Each social network, in fact, is characterised by differential peculiarities that often*

[50] The judgement provided an opportunity to analyse, through an interesting and in-depth investigation, how the requirements adopted by Article 9 l.192/1998 should be considered, avoiding a simplistic approach and having to take into account all the external circumstances arising from the external context: the reference is to C Meo, Economic dependence between collecting societies and social networks: insights in light of the Meta v. SIAE, forthcoming, (2023) AIDA, Annali Italiani del Diritto d'Autore, 20. Although it has been observed, in a dubiously critical sense with respect to what has been held by this decision, that, on closer inspection, in the case at hand the prerequisites for integrating the case of abuse of a dominant position could be lacking, nevertheless the solution could well be opposed where the right to information is relevant and in any case, for the purposes of the present case, even if the case of abuse does not arise, in any event the need remains to adopt appropriate regulatory strategies that guarantee the protection of underlying interests, including those of constitutional relevance, which cannot be abandoned to the rules of the market.

make it unattainable for the public. This is all the more true in the case under scrutiny today where one of Meta's social networks (i.e. Facebook, the notoriously more 'generalist' one) alone manages almost twice as many accounts as its main competitor'.

5. Self-regulation and co-regulation: an opportunity for efficiency of regulatory sources in the digital marketplace necessary and convenient for the platforms themselves.

In conclusion, even disregarding the technical contents of the regulation on fair compensation, even if they can be improved, in any case it would not have been appropriate to repress and nip in the bud the experimentation underway, which - if properly conducted - can lead to useful results, with a view to loyal cooperation between all protagonists, through - precisely - the '*co-regulation*', which stems from the principle of subsidiarity under Article 118 of the Constitution.

It is hoped that the EU Court of Justice, in assessing the compatibility of the fair compensation regulation with EU law, will be able to assess the importance of the case both for the implementation of the regulatory technique of *co-regulation* and for the survival of pluralism of information and thus for the protection of fundamental rights.

There is more behind this episode.

It must be adequately assessed and interpreted not only within the limits of the fair compensation regulation, since (as is also foreseen for the new front of the extended opposition to the ROC), there evidently transpires more than an '*intolerance to any form of rule*' on the part of the digital platforms, or at least some of them, as was noted by a commissioner of the AGCOM itself[51] . This is not the right approach, but, it must be reiterated, there is a need for a cultural awareness on the part of all those involved in the system (authorities, judiciary, doctrine) that these technological innovations call for new forms of regulation and settlement of opposing interests. This is first and foremost in the general interest of the market and to protect the fundamental rights of the network public, but also in the (private and individual) interest of all players. Even of the strongest, such as the digital platforms.

Therefore, some important questions arise, assuming, of course, that Mark Zuckerberg and Jeff Bezos are correctly informed that - in the small and complex European market - the Italian offices of their multinationals are pursuing these appeals[52] : are we certain that there is full awareness of the future consequences of this political strategy adopted by Meta and Amazon? Does the logic of conflict with any form of regulation by states apply equally to all countries or only to a different extent for some? Will it also be shared with

[51]https://www.huffingtonpost.it/blog/2024/02/22/news/difendere_il_regolamento_agcom_vuol_dire_difendere_la_libera_informazione-15196483/.

[52] However, the problem also arises in similar terms in other countries, as evidenced by Meta's decision to close the '*News*' section in the United Kingdom, Germany, France, Canada and Australia, as repeatedly mentioned.

the other (*over the top*) platforms that seem to have shown greater willingness to dialogue (such as Apple and Google)?

If the platforms' desire is to reject all forms of cooperation with states in an attempt to establish shared rules, then the policy of states will also end up having to take different paths in the future, no longer in a logic of cooperation, but - unfortunately - one of confrontation alone.

And this - in the long run - would not be a good outcome for the platforms either, despite the current weakness of states being unable to dictate rules in the market with respect to the economic power of the platforms themselves.

Carleo R, 'The AGCOM regulation on "fair compensation": a co-regulation model in search of efficiency / Il regolamento AGCOM sull'"equo compenso": un modello di co-regolazione in cerca di efficienza' (2023) 2 EJPLT, 20 - 55.
DOI:

EJPLT
ISSN 2704-8012



Il regolamento AGCOM sull'"equo compenso": un modello di co-regolazione in cerca di efficienza.*

ROBERTO CARLEO
Professore ordinario di Diritto privato
Università degli Studi di Napoli Parthenope
Avvocato

Abstract

Il Consiglio di Stato (n. 894/24) ha riformato il provvedimento con cui il TAR del Lazio (n. 18790/23) aveva sospeso il regolamento AGCOM sull'equo compenso, con ciò consentendo di non interrompere un importante tentativo di sperimentare la co-regolazione, al fine di trovare un punto di equilibrio in materia di libera diffusione di contenuti dei giornali on-line tra gli interessi delle piattaforme digitali, degli editori e del pubblico dei fruitori delle informazioni divulgate.

Le piattaforme digitali "over the top" sfuggono alla sovranità dei legislatori dei singoli stati territoriali di talché, per riuscire ad adottare una regolamentazione del mercato, si impone la necessità di una virtuosa collaborazione delle stesse piattaforme, in un'ottica di co-regolazione tra pubblico e privato, agevolata dal ruolo delle Authorities di settore, in applicazione del principio di sussidiarietà.

*Questo articolo è stato presentato alla conferenza internazionale "Il diritto dell'innovazione tecnologica. Jam Session internazionale tra giuristi", 8-9 marzo 2023, Fondazione Einaudi, Roma.
Comitato scientifico: Vincenzo Ricciuto (Univ. Tor Vergata di Roma), Lucilla Gatt (Univ. Suor Orsola Benincasa di Napoli), Carla Solinas (Univ. Tor Vergata di Roma), Mariló Gramunt Fombuena (Universitat de Barcelona).

© The author(s) 2023, 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: piattaforme digitali; equo compenso; co-regolazione; codici di auto-disciplina; autonomia regolamentata; diritto privato regolatorio; principio di sussidiarietà.

Sommario: 1. Piattaforme digitali *vs.* AGCOM: i ricorsi di Meta contro il regolamento sull'equo compenso e di Amazon contro il regolamento sull'organizzazione e la tenuta del R.O.C. (Registro Operatori della Comunicazione). - 2. Le perplessità suscitate dalla sentenza del TAR Lazio 12 dicembre 2023, n. 18790 (Meta c./ AGCOM), opportunamente riformata dal Consiglio di Stato (ord. 11 marzo 2024, n. 894): l'esigenza del bilanciamento dei servizi digitali con i diritti fondamentali. - 3. Le sanzioni irrogate a Google dall'autorità antitrust francese. - 4. La sentenza TAR Lazio 30 ottobre 2023, n. 16069 (Meta c./ AGCM e SIAE). - 5. Autodisciplina e *co-regolazione*: un'opportunità di efficienza delle fonti normative del mercato digitale necessaria e conveniente per le stesse piattaforme.

1. Piattaforme digitali *vs.* AGCOM: i ricorsi di Meta contro il regolamento sull'equo compenso e di Amazon contro il regolamento sull'organizzazione e la tenuta del R.O.C. (Registro Operatori della Comunicazione).

Il Consiglio di Stato (ordinanza n. 894/24 pubbl. 11 marzo 2024) ha riformato la sentenza del TAR del Lazio (sentenza n. 18790/23 pubbl. 12 dicembre 2023) nella parte in cui, accogliendo la domanda cautelare proposta da Meta Platforms Ireland Limited, aveva sospeso il regolamento AGCOM sull'equo compenso[1].

Il TAR aveva altresì operato il rinvio pregiudiziale della questione alla Corte di Giustizia UE, e nulla avrebbe potuto fare il Consiglio di Stato, adito da AGCOM, in ordine alla legittimità di tale rinvio pregiudiziale ormai operato dal giudice di prime cure, e sul quale la Corte UE dovrà pronunciarsi, a prescindere dall'opportuno annullamento della sospensione cautelare del regolamento AGCOM – che era stata disposta dal TAR.

Dunque, grazie all'intervento del Consiglio di Stato, la sperimentazione del regolamento dovrebbe poter continuare, con l'auspicio che questa battuta di arresto, che certamente ha costituito un ulteriore ostacolo, possa contribuire ad alimentare la necessaria attenzione che il problema merita.

---

* Articolo destinato al fascicolo monografico sul tema dell'equo compenso della Rivista 'Diritto ed Economia dei mezzi di comunicazione'.

[1] Regolamento in materia di individuazione dei criteri di riferimento per la determinazione dell'equo compenso per l'utilizzo online di pubblicazioni di carattere giornalistico di cui all'art. 43-*bis* della legge 22 aprile 1941 n.633, approvato con delibera n. 3/23/CONS del 19 gennaio 2023. Tale regolamento AGCOM ribadisce il D.Lgs, 12 dicembre 2021, n. 177, Attuazione della direttiva (UE) 2019/790 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (c.d. "Direttiva Copyright").
Da ultimo occorre aggiungere che, dopo la decisione del Consiglio di Stato, Meta ha nuovamente adito il TAR riproponendo ancora la istanza di sospensione del suddetto Regolamento, ma in questo caso la stessa Sezione Quarta del TAR Lazio ha prontamente respinto il ricorso cautelare, conformandosi alla decisione del Consiglio di Stato (così Tar Lazio, ord. n. 1929/24, R.G. 4893/24, pubbl. 16 maggio 2024).

In particolare, il tema rilevante è quello di come contemperare i diversi interessi che la legge, in attuazione della direttiva, considera ma non compone.

In quest'ottica, il regolamento intorno al quale verte il caso in esame potrebbe essere un modello italiano, anche da esportare, per risolvere il noto problema della difficoltà per i regolatori nazionali di imporre regole alle piattaforme digitali.

I limiti di territorialità delle leggi statali, incapaci di regolare lo spazio globale della rete[2], hanno indotto, seguendo i suggerimenti della dottrina, a sperimentare il ricorso a più moderne ed efficaci tecniche normative: l'"autodisciplina"[3], la "co-regolazione"[4] e la "regolazione partecipata"[5], tutte fondate sul principio di sussidiarietà di cui all'art. 118 Cost.[6] .

Essendo rimossa la sospensiva, la pendenza del rinvio alla Corte UE – allo stato – non dovrebbe impedire di continuare a sviluppare la auspicata sperimentazione del regolamento, che dovrebbe essere attentamente vagliato anche dalla stessa Corte di Giustizia, al fine di coglierne le potenzialità per la soluzione di un problema che sta diventando sempre più grave e urgente da risolvere non solo in Europa.

Meta Italia - opponendosi alla sperimentazione del sistema dell'equo compenso (tutt'altro che invasivo e a costo quasi irrilevante per la gigantesca dimensione e capacità della piattaforma) – ha provocato il rischio di nuocere a tutte le piattaforme che dovrebbero, invece, sviluppare i propri codici di autodisciplina e di condotta in un'ottica di leale cooperazione e non porsi - invece - in aperto contrasto con gli Stati.

E, soprattutto, le piattaforme non dovrebbero porsi anche contro quegli Stati che (come in questo caso ha fatto il nostro) - lungi dall'imporre autoritativamente rigide regole eterodeterminate - stanno tentando di

---

[2] Come già da tempo autorevolmente rilevato da N. IRTI, *Norma e luoghi, problemi di geo-diritto*, Roma-Bari, 2001

[3] Cfr A. BELLELLI, *Soft law e co-regolazione*, in *Manuale di diritto privato dell'informatica*, a cura di R. Bocchini, Napoli, 2023, p.51 ss.

[4] Cfr F. BASSAN, *Digital Platforms and Global Law*, Edward Elgar Publishing, Cheltenham, 2021; U. MALVAGNA, M. RABITTI, *Filiere produttive e Covid-19: tra rinegoziazione e co-regolazione*, in *Nuovo Dir.Civ.*, 2020, 4, p.369 ss.; M. RABITTI, *Le regole di supervisione nel mercato digitale: considerazioni intorno alla comunicazione Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, in *Riv. Trim. Dir. Econ.*, Suppl. n. 3 al n. 1/2022, p.119 ss.

[5] Cfr. F. BASSAN, *Digital Platforms and Blockchains: the Age of Participatory Regulation, in European Business Law Review* 34, no. 7 (2023): 1103-1132, il quale spiega cos'è la co-regolazione e quella che l'A. definisce "regolazione partecipata'". F. BASSAN, M. RABITTI, *Recenti evoluzioni dei contratti sulla blockchain. Dagli smart legal contracts ai 'contracts on chain'*, in diritto bancario, III, 2023, https://rivista.dirittobancario.it/recenti-evoluzioni-dei-contratti-sulla-blockchain-dagli-smart-legal-contracts-ai-contracts-chain). La 'regolazione partecipata' è una forma nuova di co-regolazione, in cui i ruoli dei regolatori e del mercato sono meno definiti e possono invertirsi, iniziando da subito la cooperazione tra operatori del mercato, regolatori e legislatori. In altri termini, mentre nei meccanismi classici della co-regolazione il procedimento comincia con le autorità che elaborano testi e proposte di regole, che poi il mercato commenta, partecipando a procedure di consultazione; invece nella 'regolazione partecipata' legislatori, regolatori e operatori collaborano sin dalla fase iniziale della realizzazione dei prodotti e dei servizi, per elaborare insieme i requisiti minimi ritenuti idonei a garantire il rispetto del *welfare* europeo continentale, cui poi il mercato dovrà conformarsi, secondo il c.d. '*circolo regolatorio'* di regole che nascono dal mercato e tornano al mercato (ovvero dapprima il mercato tende ad allinearsi alle *best practices* le quali vengono trasformate in *standard* dalle autorità nazionali, che li condividono poi nei consessi europei, trasformandoli in *standard* europei, in alcuni casi anche in '*regole tecniche'*, le quali poi a loro volta tornano al mercato. Cfr. anche nota 4 e 7.

[6] Cfr. M. NUZZO (a cura di), *Il principio di sussidiarietà nel diritto privato*, Vol. I e II, Torino, 2014.

favorire il ricorso a nuove fonti di disciplina[7] (in gran parte di *soft law*) fondate, appunto, sulla *co-regolazione*, sulla "regolazione partecipata" e sulla sperimentazione (secondo il moderno modello della *sand box* regolamentare)[8].

Che da parte delle piattaforme non ci fosse stato un approccio di "leale collaborazione" era già emerso per la manifesta irrisorietà delle offerte di equo compenso che (nella breve e sfortunata sperimentazione del regolamento) le piattaforme avevano cominciato a proporre agli editori.

Si pensi, ad esempio, alla irrisorietà delle proposte di cifre "annuali" (massimamente degradate per i giornali locali più piccoli).

Qualche dato concreto sarebbe molto eloquente per cogliere quale sia stato il livello di (in)disponibilità a negoziare manifestato dalle piattaforme in questo inizio di sperimentazione, atteso che esse hanno offerto solo pochissime centinaia di euro per anno alle testate italiane[9], e dunque tali offerte si rivelano evidentemente insufficienti per integrare i presupposti minimi di buona fede nella negoziazione[10].

Per avere contezza del ruolo sociale delle imprese editrici a garantire il pluralismo e la libertà della informazione, e quindi anche della misura dei costi sostenuti, basta considerare l'importanza del "diritto soggettivo" degli editori a ricevere il contributo pubblico all'editoria, ormai pacificamente riconosciuto come tale nella giurisprudenza ordinaria, amministrativa e costituzionale e recentemente ribadito dalle Sezioni Unite della Cassazione con la sentenza Cass. Sez. Unite, 13 maggio 2022, n. 15370[11].

Questa refrattarietà alle regole (anche di *soft law* e autodisciplina) e questa assenza di disponibilità al dialogo delle piattaforme digitali nei confronti delle parti sociali della *platform economy* determina delle gravi conseguenze in termini di sostenibilità sociale e, in qualche misura anche reputazionale e di *Corporate Social Responsibility* delle piattaforme "*over the top*" (nella specie di

---

[7] Per un'analisi del "*crescente posizionamento di altre tecniche di regolazione che vanno dalle strategie del* Nudging *a meccanismi di* Engagement*, all'automazione del diritto per effetto della tecnologia*", cfr. M. RABITTI, *Modelli partecipativi di gestione e prevenzione dei nuovi rischi di impresa tra regolazione e vigilanza*, in AA.VV., *Le clausole generali nel diritto dell'economia*, Torino, 2024, p. 143 ss.

[8] In Italia la prima norma che prevede la "*sandbox regolamentare*" è stata inserita nell'art. 36, comma 2-*bis* del D.L. 34/2019 (cd. "Decreto Crescita") delegando al Ministero dell'economia e delle finanze ("MEF") l'emanazione di uno o più decreti per regolare la sperimentazione fintech "*volta al perseguimento, mediante nuove tecnologie quali l'intelligenza artificiale e i registri distribuiti, dell'innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati*". Successivamente, in data 17 luglio 2021 è entrato in vigore il decreto attuativo del MEF, che istituisce presso di esso un Comitato *Fintech* la cui principale funzione è quella di definire gli obiettivi e mediare tra operatori del settore e autorità vigilanti, In concreto la *sandbox* italiana, sulla falsariga del modello inglese, consiste in un ambiente in cui gli operatori del settore *fintech* si confrontano con le autorità di vigilanza competenti sperimentando per un periodo di tempo limitato prodotti e servizi innovativi nel settore bancario, assicurativo e finanziario, a fronte di un regime regolamentare semplificato.

[9] Senza dubbio i parametri dell'*equo compenso* (che è un corrispettivo basato sui ricavi che le piattaforme ottengono per lo sfruttamento dei contenuti creati dagli editori) non possono essere equiparati a quelli del *contributo pubblico all'editoria* (che, invece, viene riconosciuto solo a particolari tipologie di imprese editoriali, ed è determinato in funzione di rimborso parziale dei costi sostenuti). Struttura e funzione sono diversi, e certamente non si può pretendere di porre a carico delle piattaforme il costo del sostegno pubblico all'editoria. Ciononostante la misura del contributo pubblico (laddove esiste) concorre a dimostrare l'irrisorietà delle offerte di equo compenso che le piattaforme hanno ritenuto di proporre.

[10] I medesimi presupposti minimi della buona fede sono stati invece tenuti nella doverosa considerazione dallo stesso TAR in un'altra pronuncia che ha visto Meta Italia soccombente a favore della AGCM e della Siae, sulla quale si tornerà appresso (cfr. par. 4).

[11] Sul punto cfr. per tutti A. PARISELLA, *Contributi all'editoria e diritti soggettivi*, in *Diritto ed Economia dei Mezzi di Comunicazione*, 2023, 3, p. 55 ss.

quelle più grandi, ovvero le c.d. VLOPs, *Very Large Online Platforms*), che acuiscono il rischio di inasprire inesorabilmente il problema della individuazione delle regole che queste piattaforme dovrebbero rispettare, ma che gli Stati non sono in grado di imporre, stanti i limiti della sovranità territoriale[12] .

Questo evidente potere di fatto induce a riconoscere legittimazione alla tesi secondo la quale le piattaforme più importanti possano essere qualificate in termini di "ordinamenti privati"[13], per cui è giocoforza sperimentare nuove fonti di normazione, quali, appunto, la co-regolazione o la "*regolazione partecipata*"[14].

Appare paradossale che le piattaforme, in un'ottica che appare di certo egoistica ed unilaterale, accusino gli Stati di violare la libertà di iniziativa economica imponendo delle regole che sarebbero contrarie alla libera circolazione delle informazioni.

Non si tiene in alcun conto che, invece, il tema della libertà e del pluralismo dell'informazione è delicatissimo e non può essere abbandonato esclusivamente a mere logiche di mercato.

La tutela delle libertà di informazione non è affatto un limite, ma una virtù, per cui i sostegni e gli interventi pubblici sono necessari per garantire l'art. 21 Cost.[15].

La decisione del TAR non sembrava avere adeguatamente valutato i suddetti problemi ed aveva finito per avallare lo "*strapotere delle piattaforme*", impedendo allo Stato non solo di "dettare" ma anche solo di "concorrere" alla regolazione del mercato delle informazioni.

Occorre invece tutelare e bilanciare i diritti degli editori e dei fruitori delle informazioni, che restano a rischio di essere pregiudicati dalla incontrollata ed incontrollabile dittatura delle piattaforme stesse, alle quali non potrebbe opporsi alcuna regola, nemmeno "condividendola", in contrasto con la cultura dialogica alla quale la direttiva fa espresso riferimento.

E soprattutto occorre prestare attenzione *all'interesse pubblico*, ovvero ai benefici che la disciplina dell'equo compenso può recare in favore del pubblico dei fruitori della rete che utilizzano le piattaforme, i quali potrebbero continuare a godere, attraverso la rete, dei contenuti protetti dal diritto di autore degli editori, senza oneri, ovvero gratuitamente (a prescindere qui dal noto problema della "condivisione" dei propri dati personali che le piattaforme acquisiscono)[16].

La legittimità e l'opportunità del regolamento sull'equo compenso dovrebbero essere valutate anche in considerazione del ruolo di vigilanza,

---

[12] Su cui cfr. ancora N. IRTI, *Norma e luoghi. Problemi di geo-diritto*, cit

[13] Ci si riferisce alla tesi di F. BASSAN, op. cit. (cfr. nota 4, 5 e 7).

[14] Cfr. nota 5.

[15] Cfr. ancora A. PARISELLA, op.cit. Del resto la stessa direttiva sottolinea la importanza di questo profilo, come si può evincere già dal testo del considerando 54, ove si afferma che: "*Una stampa libera e pluralista è essenziale per garantire un giornalismo di qualità e l'accesso dei cittadini all'informazione e da un contributo fondamentale al dibattito pubblico e al corretto funzionamento di una società democratica*".
Con particolare riferimento proprio all'importanza della disciplina dell'equo compenso introdotta dalla direttiva europea in materia di *copyright* nell'obiettivo di sostenere il pluralismo dell'informazione si rinvia ad A. PAPA, *La tutela del pluralismo informativo in Rete. Il ruolo e le prospettive della direttiva europea 2019/790*, in AA. VV*., Il diritto d'autore nell'era digitale*, a cura di A. Papa, Torino, 2023, 2019, p. 13 ss.

[16] Sul punto, cfr. per tutti C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, V. RICCIUTO, *L'equivoco della* privacy. *Persona* vs *dato personale*, Napoli, 2022.

controllo e regolazione del mercato della diffusione *on line* dei contenuti informativi degli editori svolto dall'AGCOM. In quest'ottica l'AGCOM, nel libero mercato delle comunicazioni, che tuttavia, nel rispetto della legge, può e deve essere regolamentato dall'autorità a ciò preposta nel nostro ordinamento[17], è tenuta a realizzare un bilanciamento non solo degli interessi (privati) delle piattaforme e degli editori, ma anche dell'interesse generale dei fruitori delle informazioni.

Il problema si sta riproponendo con un bersaglio ancora più grave e importante rispetto al regolamento sull'equo compenso: le piattaforme mirano adesso a contestare persino il R.O.C. (Registro Operatori della Comunicazione, tenuto dall'AGCOM, che costituisce un sistema più moderno ed evoluto rispetto alla antica iscrizione delle testate giornalistiche presso i Tribunali, che era storicamente ispirata alla ormai superata logica del contrasto alla stampa clandestina). Le piattaforme mostrano, quindi, di rifiutare anche di assoggettarsi a quelle minime forme di tributo e controllo necessarie per gestire il registro pubblico degli "operatori della comunicazione", utilissimo a garanzia della qualità e della affidabilità della informazione ed alla tutela del pluralismo.

Amazon ha già presentato questo ricorso, come del resto aveva preannunciato in sede di consultazione[18].

Di talché è a rischio anche quest'altro (piccolo) paletto - il R.O.C. - con cui si potrebbe tentare una qualche attività di regolazione del mercato della comunicazione in cui hanno fatto irruzione le piattaforme digitali, sempre più potenti (con gli Stati sempre più deboli).

2. Le perplessità suscitate dalla sentenza del TAR Lazio 12 dicembre 2023 n. 18790 (Meta c./ AGCOM), opportunamente riformata dal Consiglio di Stato (ord. 11 marzo 2024, n. 894): l'esigenza del bilanciamento dei servizi digitali con i diritti fondamentali.

L'approccio che il TAR aveva condiviso in questa vicenda del regolamento sull'equo compenso favoriva lo strapotere aggressivo delle piattaforme, che, tra l'altro, attualmente stanno de-indicizzando i siti dei giornali e tendono ad abbandonare la costruzione delle notizie, affidandola - invece - alla incontrollata composizione da parte dei sistemi della intelligenza artificiale c.d. "generativa"[19].

Ecco allora - tra le inevitabili conseguenze della alimentazione di un conflitto tra posizioni antitetiche, senza tentativi di mediazione - la conseguenza che il

[17] Contro le pretese di naturalità, nel senso che il mercato consiste nello "statuto di regole" create dal legislatore (anche quando sceglie di non intervenire) e quindi è sempre *locus artificialis*, cfr. N. IRTI, *L'ordine giuridico del mercato*, Roma-Bari, 1998.

[18] Cfr. Allegato 1 alla delibera n. 270/23/CONS contenente la Sintesi delle osservazioni alla consultazione pubblica in merito alla proposta di modifica del Regolamento per l'organizzazione e la tenuta del Registro degli operatori di comunicazione, in https://www.agcom.it/documents/10179/32496245/Allegato+28-11-2023/1e3b1174-cde9-4054-83b6-90ab7f99b5fc?version=1.0.

[19] In ordine alle conseguenze economiche legate ad uno sviluppo incontrollate di tali sistemi v. S. DA EMPOLI, *L'economia di ChatGPT. Tra false paure e veri rischi*, Milano, 2023, p. 53 ss.

glorioso quotidiano *New York Times* ha citato in giudizio OpenAI, Microsoft (ed altri) diffidando *ChatGPT* dall'uso dei suoi contenuti[20].

Non è questa la sede per soffermarci sulla questione che si pone al centro di un dibattito, assai intenso negli Stati Uniti (e non solo), che si incentra sull'analisi dell'attività di elaborazione di opere intellettuali mediante l'uso di intelligenza artificiale[21], chiedendosi se essa sia o non sia creativa, e, di conseguenza, se sia o non sia soggetta alla protezione del diritto d'autore; invero, a prescindere da come venga risolta la questione, essa consente di ribadire con certezza che i vari modi di utilizzo dei contenuti dei giornali (siano essi suscettibili o meno di protezione del diritto d'autore) rappresentano evidentemente un ingiustificato arricchimento delle piattaforme digitali in danno ai giornali stessi, i quali - in ragione di questo *trend* - finiranno per scomparire, pregiudicando, altresì, gravemente il pluralismo e l'indipendenza dell'informazione.

È notizia recente che Meta ha chiuso in Regno Unito, Germania e Francia (ovvero nei paesi europei in cui il servizio era stato attivato, tra i quali l'Italia non è mai stata inclusa), e poi anche in Canada ed in Australia, la propria sezione "*News*", con ciò – di fatto – rifiutandosi di veicolare i contenuti dei giornali. Posto che proprio questi paesi (come si vedrà)[22] si sono dotati o stanno tentando di dotarsi di una legislazione in materia, volta a considerare le piattaforme *online* al pari di ogni altro editore di contenuti e di conseguenza assoggettarle a tassazione o ad altre regole, si evince che la politica di queste piattaforme "*over the top*", non solo in Italia, rischia di porsi in aperto contrasto contro qualsiasi regola[23].

---

[20] Domanda n. 1:23-cv-11195 del 27 dicembre 2023 proposta dinanzi alla United States District Court for the Southern District of New York, courthousenews.com. Cfr. anche nota 38.

[21] Cfr J.C. GINSBURG, *Fair use in the United States: transformed, deformed, reformed?,* in *Singapore Journal of Legal Studies*, marzo 2020, 265-294, reperibile anche *online* al seguente indirizzo: https://law1.nus.edu.sg/sjls/articles/SJLS-Mar-20-265.pdf; J.C. GINSBURG, L.A. BUDIARDJO, *Authors and Machines*, in *Berkeley Technology Law Journal*, 2019, vol.34, n.2, 358 ss., reperibile anche *online*: https://lawcat.berkeley.edu/nanna/record/1136665/files/01_Ginsburg_Web%5B1%5D.pdf?withWatermark=0&withMetadata=0&version=1&registerDownload=1

[22] Cfr. par. 3.

[23] I termini ed i rischi del problema per la sopravvivenza dei giornali sono messi in luce, con lucida e cruda chiarezza, da V. GHIONNI, *Facebook e l'equo compenso: la discussione sul nulla*, in https://www.editoria.tv/facebook-e-equo-compenso-la-discussione-sul-nulla/, 2 marzo 2024, il quale osserva che: "*Il contenzioso tra Meta e l'Autorità per le garanzie nelle comunicazioni circa l'applicazione della legge sull'equo compenso è seguita con grande attenzione dai giornali. La Fieg si associa al ricorso dell'Autorità, applaude, sorride e ringrazia. Meta ritiene di non dover essere assoggettata alla regolamentazione italiana e il Tar gli dà ragione. Si discute, si dibatte, basti pensare che dalla Direttiva comunitaria che ha previsto l'equo compenso a favore degli editori alla delibera dell'Autorità sono passati quasi quattro anni. In questo periodo gli editori di giornali hanno perso milioni di copie e gli over the top hanno guadagnato miliardi di euro, hanno affinato gli algoritmi, rafforzato ulteriormente la loro centralità nel mercato e nella capacità di influenzare l'opinione pubblica. La ratio dell'equo compenso è quello di riequilibrare il mercato, sottrarre un po' a chi pubblica i contenuti per dare qualcosa a chi li produce. Nel 2019, anno di emanazione della delibera comunitaria, l'intelligenza artificiale era ancora fantascienza, oggi è realtà. Non c'era la guerra in Ucraina che ha ulteriormente polarizzato il dibattito, i contenuti erano ancora un valore. Ma intanto che i tribunali decidono, gli editori plaudono e i soloni dibattono, Meta continua a macinare utili, gli editori perdono copie e fatturato. Gli unici che stanno tranquilli rimangono i soloni tanto c'è sempre un coffee break o un light lunch tra un simposio ed un seminario. E qualcuno che applaude. Poi arrivano notizie da oltre oceano che destano scalpore, Meta chiude le sezioni news in Australia e negli Stati Uniti. Peccato che già l'aveva fatto qualche mese fa in Francia, Regno Unito e in Germania, i contenuti degli altri non gli servono più, ci sta l'intelligenza artificiale diventata intanto realtà e allora perché buttare soldi da dare ai giornali che poi l'algoritmo ubbidisce al padrone meglio del più paludato cronista. Tra qualche mese il Consiglio di Stato deciderà nella querelle Meta-AgCom, sarà passato altro tempo, i giornali avranno continuato*

In buona sostanza, pur di non accettare di sottoporsi a regole (sia pure condivise), Meta ha deciso di invertire la propria politica di divulgare i contenuti informativi, estromettendoli dalla propria piattaforma.

Ma per questa via si acuisce il conflitto con gli Stati e si danneggiano gli stessi fruitori dei contenuti.

Il problema (come in Italia già è accaduto per la musica)[24] potrebbe ritorcersi contro le stesse piattaforme, laddove si ritenesse che la piattaforma in questione (in questo caso Facebook) abbia assunto una tale importanza come veicolo di circolazione *on line* anche dei contenuti informativi[25], tanto da non essere fungibile in mancanza di altri strumenti equipollenti e quindi da essere obbligata a veicolare tutti i contenuti, senza poterli escludere, quasi alla stregua di un *monopolista di un servizio pubblico digitale*.

Questi rapidi cenni appaiono già determinanti al fine di farci meditare sull'importanza di sperimentare la disciplina dell'equo compenso, che potrebbe contribuire a realizzare (non solo in Italia) un punto di equilibrio "condiviso" tra diritti delle piattaforme, degli editori e - soprattutto - degli utenti delle informazioni.

Non è forse meglio concordare un punto di incontro tra diritto d'autore e diffusione libera dei contenuti nella rete, così come la disciplina della costruzione di un equo compenso agli editori mira a realizzare?

La logica della contrapposizione fra parti che operano in un contesto caratterizzato dalla complessità non sembra condurre lontano, e sembra invece aggravare problemi già difficili da risolvere.

Occorre che tutti i protagonisti sociali – autorità, magistratura, dottrina – siano culturalmente preparati a comprendere ed affrontare il problema delle nuove tecnologie e delle nuove fonti del diritto che inevitabilmente devono impiegarsi.

Certamente le piattaforme, alla luce del contesto in cui operano, non sono "parte debole". Appare un po' anomalo che il TAR abbia affermato (anche più volte) che esse sarebbero addirittura in una situazione di "*soggezione*"[26].

Uno dei punti della sentenza che destava maggiori perplessità si può rinvenire nella qualificazione del meccanismo di co-regolazione alla stregua di un "*arbitrato obbligatorio*".

---

a perdere copie e fatturato e Meta a guadagnare e incrementare la capacità di condizionare l'opinione pubblica. Se perderà nelle sedi giudiziarie disattiverà la sezione news anche in Italia. E sarà argomento per i Soloni."

[24] Cfr. par. 4.

[25] Non a caso nel comunicato con cui la stessa Meta annuncia la dismissione del servizio, si premura di giustificare la propria decisione adducendo lo scarso successo delle *news* sul *social*: "*Le persone non vengono su Facebook per leggere notizie e contenuti politici ma per connettersi con gli altri e scoprire nuove opportunità, passioni e interessi. Le notizie rappresentano meno del 3% di quanto viene visto sui feed di Facebook, una piccola parte di un'esperienza molto più ampia per la stragrande maggioranza degli utenti*". Il colosso dei social ci tiene altresì a precisare che le modifiche che interessano *Facebook News* non avranno alcun impatto sui prodotti e servizi di Meta in questi Paesi e le persone potranno comunque visualizzare i collegamenti agli articoli di notizie su Facebook. Gli editori di notizie continueranno ad avere accesso ai propri *account* e alle proprie pagine Facebook, ove potranno pubblicare collegamenti alle loro storie e spingere le persone a visitare i loro siti Web, nello stesso modo in cui può farlo qualsiasi altro individuo o organizzazione.
Inoltre, le testate giornalistiche potranno anche sfruttare prodotti come *Reels* e il sistema pubblicitario di Meta per raggiungere un pubblico più ampio e indirizzare le persone ai loro siti Web.

[26] Cfr. pag 23 e 27 della sentenza richiamata (sebbene prive di numerazione).

Dopo una tale affermazione, nelle pagine successive si parla, invece, di "*arbitraggio*" (cfr. pag. 26 s), aumentando così la confusione delle qualificazioni della fattispecie mediante il richiamo all'art.1349 c.c.[27].

Il TAR aveva affermato (cfr. pag. 6) che "*l'art. 43-bis L.a. (e, quindi, la Delibera è il Regolamento che lo implementano) ha introdotto un diritto di remunerazione (equo compenso) suscettibile di essere interpretato come (o, comunque, sostanziato dalla introduzione di fatto di) un 'obbligo di negoziare', che limita significativamente la libertà contrattuale degli operatori economici ed al quale accede un 'obbligo di pagamento'*".

Inoltre aveva affermato (cfr. pag.7 s.) che tali nuovi interventi normativi sarebbero "*contrari alla libertà d'impresa*" poiché implicherebbero: 1) una determinazione delle tariffe ed una previsione di una "*procedura di arbitrato obbligatoria*" (che reintrodurrebbe, di fatto, una forma di determinazione autoritativa dei prezzi dei prodotti liberamente scambiati sul mercato); 2) una "*significativa limitazione della libertà contrattuale*"; 3) un obbligo di non limitare la visibilità nei risultati della ricerca durante le negoziazioni (in violazione della EUCD e della Legge delega, che non prevedono alcuna norma di questo tipo); 4) un "*ruolo affidato ad Agcom*" (cui una delle parti potrebbe rivolgersi durante le trattative per attivare una procedura di determinazione del compenso); 5) "*criteri sproporzionati e discriminatori da considerare per determinate l'equa remunerazione*" (quali sarebbero il numero di giornalisti impiegati e la rilevanza dell'editore, criteri contestati anche in un parere dell'AGCM); 6) "*obblighi di messa a disposizione di dati*" (a carico degli ISSP, su richiesta della parte interessata o di AGCOM), con rinvenimento potere sanzionatorio di quest'ultima; 7) "*poteri ispettivi*" riconosciuti ad AGCOM (per acquisire i parametri necessari per la determinazione dell'equo compenso); 8) "*obblighi di messa a disposizione di dati privi di base giuridica, sproporzionati e in contrasto con la EUCD*".

Addirittura, secondo il TAR, ricorrerebbero persino violazioni di principi costituzionali, come la libertà della iniziativa economica, i principi di proporzionalità e ragionevolezza, il principio di uguaglianza e non discriminazione (per il beneficio "*irragionevole*" concesso ai soli editori).

Ma questa decisione trascurava completamente la fonte della "co-regolazione" e la "autonomia regolamentata", che è alla base del moderno "diritto privato regolatorio"[28].

E mancava soprattutto l'attenzione al *pubblico* che beneficia dei contenuti diffusi dalle piattaforme.

Questo è un interesse del mercato che lo Stato deve tutelare e prediligere.

La piattaforma digitale, invece, non è un soggetto debole da tutelare in una "trattativa privata".

E l'autorità non è affatto un "*contraente forte*" che agisce nel proprio interesse, bensì un soggetto pubblico che - appunto nell'interesse pubblico - deve poter esercitare i suoi poteri di controllo e anche sanzionatori.

---

[27] Sul punto - per la chiara e nota distinzione tra *arbitri*, che decidono controversie giuridiche, e *arbitratori*, che determinano il contenuto economico di un contratto - resta tuttora attuale e fondamentale il rinvio a F. CARNELUTTI, *Arbitri e arbitratori*, in *Riv.dir.proc.*, 1924, p.6 ss.

[28] Cfr. A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020; M. ANGELONE e M. ZARRO (a cura di), *Diritto civile della regolazione: conformazione degli atti di autonomia e disciplina dei mercati*, Napoli, 2022.

Non si vuole negare che il regolamento sull'equo compenso, varato dall'AGCOM il 19 gennaio 2023, sulla base del D. Lgs 177/21 attuativo della direttiva (UE) 2019/790 [29], possa essere suscettibile di miglioramenti, o revocare in dubbio che trovino ragione di porsi dei problemi di compatibilità della disciplina di recepimento con la direttiva europea.

Tuttavia la stessa direttiva Copyright (in particolare dell'art.15 "*Protezione delle pubblicazioni di carattere giornalistico in caso di utilizzo online*") e la sua attuazione tramite la disciplina italiana dell'equo compenso di cui qui si discute devono necessariamente essere interpretate alla luce di tutte le libertà fondamentali tutelate dalla Carta dei diritti fondamentali dell'Unione europea (CDFUE), dalla CEDU e anche dalla nostra Costituzione (e innanzitutto della libertà di informazione di cui all'art. 11 CDFUE, 10 CEDU e 21 Cost.[30], che peraltro è proprio nelle finalità della direttiva stessa che mira a tutelare il diritto d'autore), di talché non può trascurarsi di considerare il bilanciamento di tutti gli interessi in gioco, limitandosi invece ad un'isolata attenzione solo di alcuni profili di regole del mercato e della libertà di iniziativa economica.

Del resto, oggi il bilanciamento delle regole di prestazione dei servizi digitali con i diritti fondamentali è espressamente imposto dall'art. 14 del *Digital Services Act* (con l'obiettivo di migliorare la moderazione dei contenuti sulle piattaforme dei social media per affrontare le preoccupazioni sui contenuti illegali)[31], e di ciò la Corte di giustizia europea certamente dovrà tenere conto, così come (oltre che del suddetto DSA) anche della direttiva sui servizi di media audiovisivi (*Audiovisual Media Services Directive, AVMSD*)[32], del Digital Market Act (DMA)[33] e del recentissimo *European Media Freedom Act (EMFA)*, approvato dal Parlamento Europeo lo scorso 13 marzo 2024, finalizzato a proteggere i media europei da ingerenze politiche o economiche, a tutela proprio del diritto all'informazione, con particolare attenzione alle insidie generate dalla digitalizzazione[34].

---

[29] Cfr. nota 1.

[30] La rilevanza di tali principi si riscontra anche nell'art. 2 TUE che, nel richiamare i valori fondanti dello stato di diritto, richiama anche il pluralismo. Sulla essenzialità della libertà di stampa per la democrazia, cfr., nella prospettiva della regolazione europea, R. MASTROIANNI, *Freedom and pluralism of the media: an European value waiting to be discovered?*, *Medialaws*, 1, 2022, p. 100 ss. Risalendo alle origini, non si possono non richiamare le celebri pagine di J. MILTON, *Areopagitica, Discorso per la libertà della stampa*, Traduzione e prefazione di S. Breglia, Bari, 1933 (rist. in *Diritto ed Economia dei Mezzi di Comunicazione*, 2021,2).

[31] L'art. 14 del DSA (Normativa sui servizi digitali, approvato come Regolamento UE 2022/2065, finalizzato a "*contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione ed in cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo*") muove un primo passo importante nell'ottica del c.d. *costituzionalismo digitale*, cioè l'adattamento dei valori costituzionali alle peculiarità dell'ambiente digitale. Infatti il DSA introduce un obbligo di considerare nell'attuazione e applicazione dei termini di servizio anche i diritti fondamentali dei cittadini ("incorporare i diritti fondamentali nei TOS"), in particolare la libertà di espressione e il pluralismo dei media. Inoltre è espressamente previsto che le piattaforme debbano agire in maniera diligente e proporzionata, e non arbitraria né discriminatoria.

[32] Direttiva (UE) 2018/1808 del Parlamento Europeo e del Consiglio del 14 novembre 2018, finalizzata a garantire il corretto funzionamento del mercato unico digitale nella UE per i servizi di media audiovisivi, contribuendo nel contempo alla promozione della diversità culturale e fornendo un livello adeguato di protezione dei consumatori e dei minori.

[33] Regolamento (UE) 2022/1925, finalizzato a garantire che i mercati digitali nei quali sono presenti *gatekeepers* (controllori dell'accesso) siano equi e contendibili in tutta la UE.

[34] Con tale atto normativo – nel quale si segnala una accresciuta consapevolezza della esigenza di implementare la cooperazione tra le autorità nazionali competenti per contrastare la frammentazione normativa e quindi di ricorrere alla co-regolazione, fondata sul dialogo con le piattaforme più rilevanti (le

La rapidità della rivoluzione digitale e l'impatto sul mondo della informazione e dell'editoria impone una soluzione immediata per rendere compatibile l'avvento della diffusione *on line* tramite le piattaforme dei contenuti prodotti dai giornali.

L'AGCOM veniva sollecitata ad una adozione tempestiva soprattutto dagli editori che chiedevano una rapida soluzione del problema[35] (e il regolamento sull'equo compenso ha raccolto anche consensi e stimoli costruttivi)[36].

Alle voci dissenzienti, peraltro, si era annoverata anche la AGCM, che aveva espresso un parere negativo (più volte richiamato nella sentenza del TAR) rinvenendo profili di violazione dei principi della libertà della iniziativa economica e della libera concorrenza, i quali sarebbero pregiudicati da questa disciplina che imporrebbe alle piattaforme di versare l'equo compenso agli editori.

Persino dall'interno della stessa AGCOM si era levata la voce di una commissaria che non aveva mancato di esternare il proprio dissenso rispetto alla delibera del collegio di cui fa parte, sempre ritenendo che sarebbe stato imposto alle piattaforme un "obbligo di comprare"[37].

Il Consiglio di Stato ha messo ordine chiarendo che il Regolamento AGCOM non introduce alcun obbligo di negoziazione, bensì "*prevede, di fatto, un meccanismo per giungere ad un accordo, ma resta ferma la facoltà di adire il giudice competente*" (cfr. p. 16).

Ma il punto è che non si tratterebbe qui della introduzione di un semplice obbligo di negoziare imposto a soggetti privati nel libero mercato, bensì di una

---

quali, ai sensi dell'art. 17, devono rendere una dichiarazione in cui, tra l'altro, attestano di essere indipendenti e di operare conformemente ai meccanismi co-regolatori e auto-regolatori) – tra le varie novità, viene introdotto un meccanismo che mira a impedire alle *VLOPs* (*Very Large Online Platforms*), ovvero alle piattaforme digitali più grandi, di limitare o rimuovere in modo arbitrario contenuti di media indipendenti. Si chiede infatti alle grandi piattaforme *online* di distinguere i media indipendenti dalle fonti non indipendenti e di lasciare loro 24 ore per rispondere prima di eliminare i contenuti. Una volta decorso tale periodo di tempo le piattaforme potranno procedere con la rimozione e i media potranno fare ricorso rivolgendosi a un organismo per la risoluzione extragiudiziale delle controversie. I media potranno anche richiedere il parere del comitato europeo per i servizi di media, (composto da regolatori nazionali) istituito dalla nuova legge (cfr. art. 8). La direzione, dunque, è quella di evitare che le piattaforme possano escludere o "tagliare fuori" dai propri canali digitali i contenuti dei giornali i quali, viceversa, devono essere necessariamente diffusi attraverso di esse.

[35] Cfr. articolo su "Repubblica" del 15.12.2022, *Il recepimento della direttiva Ue. Gli editori: l'Autorità approvi il regolamento sul copyright. Attesi da 10 mesi i criteri per i compensi di chi produce contenuti condivisi sul web*.

[36] Cfr., ad esempio, M.L Bixio, V. Falce, *Brevi note sul principio di "fair remuneration" e "fair contract" nella Direttiva Copyright*, in *Rivista di diritto industriale*, 2020, fasc. 4-5, pt. 1, pp. 261-288; V. Falce, G. Ghidini, *Copyright digitale, il decreto non va annacquato*, in *Corriere della sera*, 3 agosto 2021, i quali, osservano, con riferimento al recepimento italiano della Direttiva, che: "*Lodevolmente, la bozza italiana di decreto prevede, per assicurare l'effettività della norma, una procedura negoziata tesa a promuovere un accordo di «buona fede» tra editori e piattaforme — come quello già stipulato fra Google e Cairo Editore. In caso di stallo, ciascuna delle parti potrà rivolgersi ad AgCom per la fissazione del prezzo. Una sorta di dialogo regolatorio, insomma, in cui ad AgCom, oltre al ruolo di arbitratore, spetta il compito di definire criteri certi ed equi della negoziazione (fra i principali, diremmo: la diversa tiratura dei giornali chiamati in causa e la diversa «autonomia informativa» dei brani «appropriati»). La bozza che andrà in consiglio dei Ministri è solida e come tale merita di uscirne senza contaminazioni e annacquamenti*"; Cfr. anche il fascicolo n. 1/23 della Rivista "*Diritto ed Economia dei mezzi di comunicazione* ", interamente dedicato al decreto legislativo 8 novembre 2021, n. 177 in tema di equo compenso a favore delle imprese editrici, che si apre con l'editoriale di A. Di Amato, *Riuscirà l'equo compenso a contrastare il declino dei giornali?*. Cfr., tra gli altri commenti contenuti nel medesimo fascicolo, V. Ghionni, *Gli impatti del decreto legislativo sulle imprese editoriali*, p. 57 ss.

[37] Così E. Giomi, *Il ricorso di Meta al Tar mette in luce le fragilità del regolamento Agcom*, in https://www.huffingtonpost.it/blog/2024/02/15/news/il_ricorso_di_meta_al_tar_mette_in_luce_alcune_fragilita_del_regolamento_agcom-15142916/.

tutela del mercato volta a proteggere gli editori e il diritto all'informazione cercando nuovi criteri di equilibrio e bilanciamento nell'interesse generale.

Occorre considerare che la disciplina dell'equo compenso mira a contemperare gli interessi degli editori che producono i contenuti, che vengono inglobati dalle piattaforme che li utilizzano divulgandoli (anche se modificati e innovati) al pubblico dei fruitori.

Non solo le piattaforme non possono arricchirsi utilizzando indebitamente i contenuti creati da altri autori, ma esse devono essere altresì tenute ad acquisirli – versando un equo compenso agli editori che li hanno generati – procedendo quindi a diffonderli a vantaggio dei fruitori attraverso i loro canali digitali, divenuti ormai essenziali ed infungibili nel mercato.

La tutela del diritto all'informazione esige dunque da un lato che le piattaforme acquistino, ma, dall'altro, anche che gli autori consentano la divulgazione dei contenuti informativi; di talché anche gli editori, venendo remunerati dall'equo compenso, non possono impedire che i propri contenuti vengano utilizzati a beneficio del pubblico che fruisce dei servizi delle piattaforme.

Ed è per questo che l'equo compenso si rivela un vantaggio anche per le piattaforme e per il pubblico dei fruitori, che non vengono privati di conoscenze che devono essere rese "comuni" per la completezza della conoscenza e della circolazione dei dati su cui si fondano i sistemi di intelligenza artificiale creativa da parte delle piattaforme stesse[38].

---

[38] Il funzionamento della disciplina dell'equo compenso, dunque, potrebbe impedire il rischio dell'insorgenza di controversie come quella attualmente in corso tra il *New York Times* ed *Open AI - ChatGPT* (cfr. nota 20), che peraltro si va allargando dato che anche altri otto giornali statunitensi di proprietà del fondo di investimento *Alden Global Capital* (tra cui il *New York Daily News* e il *Chicago Tribune*) hanno citato in giudizio Open AI e Microsoft per la stessa ragione, ritenendo che le piattaforme debbano "*ottenere il consenso degli editori per l'utilizzo dei loro contenuti e pagare un valore equo per tale utilizzo*". Ciò sebbene in altri casi la stessa *Open AI* stia mostrando di avere iniziato a stringere accordi con grandi gruppi editoriali (tra cui *Associated Press*, *Shitterstock* e in Europa il gruppo tedesco *Axel Springer*, quello spagnolo *Prisa-Promotora de Informaciones*, e il più importante giornale francese *Le Monde*).
Il risultato da evitare è il conflitto, che veda soccombente una qualsiasi delle parti: tanto il produttore del contenuto che resterebbe privato di un qualsiasi compenso, quanto la piattaforma che non potrebbe utilizzarlo. Tale ipotesi si è peraltro già verificata, ad esempio, nel caso occorso negli Stati Uniti alla piattaforma (che era una semplice *start up*) che gestiva un sistema di intelligenza artificiale "predittiva" *Ross intelligence AI*, la quale ha chiuso a fronte della minaccia del contenzioso del titolare della privativa sulla banca dati giuridica utilizzata per il funzionamento del sistema, che – pertanto - ha inesorabilmente cessato di esistere (cfr. https://www.law.com/therecorder/2023/12/15/thomson-reuters-v-ross-intelligence-ai-copyright-law-and-fair-use-on-trial/).
Il problema è ben chiaro agli analisti consulenti del governo americano, come si legge in G. PELLICANO, *C'è una via transatlantica all'IA? La proposta di Pellicano*, in Formiche.net (https://formiche.net/2024/03/intelligenza-artificiale-pellicano/) il quale rileva che "*Ulteriori ricadute dell'utilizzo dell'intelligenza artificiale riguardano il rispetto dei dati coperti dal copyright e la definizione del concetto di fair use, vale a dire l'uso limitato e lecito di materiali coperti dal diritto d'autore. La recente iniziativa del* New York Times *di chiamare in giudizio OpenAI per l'utilizzo illecito dei propri archivi finalizzato al training dell'AI potrebbe portare alla fissazione giurisprudenziale o transattiva di nuovi limiti all'utilizzo dei testi coperti da copyright. Anche in questo caso la soluzione può venire da una decisione imposta dall'autorità pubblica o da un accordo tra le parti che possa aprire le porte all'autoregolamentazione condivisa tra aziende aventi interessi contrapposti. Un'analisi efficace della posta in gioco per editori e programmatori di intelligenza artificiale è stata pubblicata a ottobre da Colombia Journalism Review: An AI engine scans a book. Is that copyright infringement or fair use?*".
Del resto, sta acquistando sempre maggiore diffusione e consapevolezza la cultura della avversione contro le forme di protezione troppo restrittive delle opere creative nell'era della digitalizzazione, che esige una condivisione globale dei dati. Tra i più attivi esponenti di tale movimento di pensiero si veda ad esempio C. DOCTOROW, il quale nella propria biografia (pubblicata sul suo sito "*Creative Commons*" già dal 2006), dichiara: "*credo che viviamo in un'epoca in cui tutto ciò che può essere espresso come bit lo sarà. Credo che i bit esistano per essere copiati. Pertanto, credo che qualsiasi modello di business che dipenda dal fatto che i bit non vengano*

Con l'equo compenso si consente alle piattaforme il beneficio di "*ingerire*" anche dati coperti dalla privativa.

La completezza dei dati è essenziale per la conoscenza[39] e dunque per il funzionamento dei sistemi di AI che funzionano elaborandoli.

Pertanto occorre bilanciare il meccanismo di *opt-out*, ovvero la facoltà per i titolari dei diritti di privativa di escludere l'utilizzo dei propri contenuti[40], con l'esigenza delle piattaforme di acquisirli nell'interesse pubblico (dunque non per le proprie finalità commerciali): e la disciplina dell'equo compenso mira proprio a raggiungere questo obiettivo.

Per questo conviene anche alle piattaforme cercare il giusto equilibrio per bilanciare gli interessi di tutti.

Altrimenti si esaspera un conflitto non solo con gli editori (che rischiano di estinguersi, pregiudicando così la libertà ed il pluralismo dell'informazione), ma anche con il pubblico dei fruitori e quindi con gli Stati, con i quali le piattaforme non dovrebbero rifiutare il dialogo.

E a ben vedere il conflitto, alla lunga, non conviene a nessuno. Nemmeno alle piattaforme.

Limitandoci a ricordare l'uso di una terminologia, la quale tuttavia può essere destinata ad assumere significato specifico diverso nei diversi contesti, basta ricordare, in via generale, che l'"*obbligo di negoziare*" è ormai entrato anche nel codice contratti pubblici (cfr. art. 9 D.Lgs n. 36/2023 che prevede il principio di conservazione dell'equilibrio contrattuale, da cui deriva - appunto - l'obbligo di contrarre e l'implementazione nei contratti pubblici delle clausole di rinegoziazione).

Anche la stessa nozione di "*equo compenso*", non sconosciuta nella legislazione del diritto d'autore[41] e variamente impiegata nel nostro ordinamento (cfr. art. 1526 c.c. in materia di equo compenso dovuto al venditore in caso di inadempimento del compratore nella vendita a rate e L. 21 aprile 2023, n. 49 in materia di equo compenso delle prestazioni professionali)

---

copiati sia semplicemente stupido, e che i legislatori che cercano di sostenerli siano come i governi che investono fortune per proteggere le persone che si ostinano a vivere alle pendici dei vulcani attivi" (cfr. https://wiki.creativecommons.org/wiki/Case_Studies/Cory_Doctorow).

[39] E. OSTROM, C. HESS, *La conoscenza come bene comune*, (2007) ed. it. Milano, 2009. Cfr. anche P. SPRINGHETTI, *L'informazione è un bene comune. Riflessioni sulla mediaetica*, Ucsi, 2013, P. AIGRAIN, *Causa comune. L'informazione tra bene comune e proprietà*, Stampa alternativa, 2007. Con specifico riferimento ai problemi della libera utilizzazione dei contenuti esclusi dagli autori nei sistemi di intelligenza artificiale cfr. Cfr. GINA MARIA ZIAJA, *The text and data mining opt-out in Article 4(3) CDSMD: Adequate veto right for rightholders or a suffocating blanket for European artificial intelligence innovations?*, in *Journal of Intellectual Property Law & Practice*, Volume 19, Issue 5, May 2024, Pages 453–459, https://doi.org/10.1093/jiplp/jpae025.

[40] Il principio dell'*opt-out* è recepito dall'AI Act europeo (approvato lo scorso 13 marzo 2024) e sarebbe in procinto di essere condiviso anche nel nuovo schema di DDL recante disposizioni e delega al Governo in materia di Intelligenza Artificiale (approvato dal Consiglio dei Ministri lo scorso 23 aprile 2024), che contiene – tra le altre - disposizioni in materia di diritto d'autore (eliminando l'obbligo di indicazione della fonte e imponendo ai media di "bollinare" i contenuti generati o modificati tramite AI per renderli riconoscibili dagli utenti).

[41] Per un'analisi dei vari precedenti nel diritto italiano, cfr. L. ATTOLICO, *L'equa remunerazione degli autori e artisti per lo sfruttamento delle proprie opere ed esecuzioni nel mercato digitale: novità e prospettive alla luce della nuova direttiva in materia di* copyright, in *Il diritto d'autore nell'era digitale*, cit., p. 87 ss.

In particolare agli artt. 70 ss. della Legge sul diritto d'autore, è stabilito che i dati coperti da diritto d'autore possono essere liberamente utilizzati – purché non a scopo di lucro ma per uso didattico o scientifico o di critica o discussione (senza costituire concorrenza alla utilizzazione economica dell'opera) – rinviando a regolamenti che fissano "*la modalità per la determinazione dell'equo compenso*" (cfr. art. 70, comma 2, L. 633/1941).

meriterebbe ulteriori approfondimenti, anche in ordine alla sua determinazione giudiziale, che potrebbe integrare ben altro rispetto ad un obbligo di "comprare" o di imporre un "prezzo".

A ben vedere, qui l'equo compenso (il cui *quantum* non è un diretto corrispettivo riferito alla sola utilità economica) esula da una logica semplicemente negoziale, ma costituisce una *misura compensativa necessaria per il corretto funzionamento del mercato*, la cui determinazione, invece che essere immediatamente ed autoritativamente imposta, si vorrebbe tentare di rimettere, auspicabilmente, ad una condivisione tra i protagonisti, sotto l'egida dell'autorità competente.

Il punto non è tanto quello di negoziare tra le parti un corrispettivo in base a parametri di mercato[42], quanto quello di trovare un criterio di equilibrio che garantisca il mercato tutelandone tutti i protagonisti, quasi alla stregua di una "tassa" imposta a carico del soggetto che realizza il maggior profitto[43].

Insomma, la direzione che il legislatore italiano ha intrapreso per recepire la direttiva, seppure suscettibile di essere affinata e perfezionata, appare utile per sperimentare le nuove fonti normative della *co-regolazione* e del ruolo delle autorità indipendenti nell'instaurare e coltivare il necessario dialogo con le piattaforme *over the top* al fine di condividere regole idonee a bilanciare i contrapposti interessi e a garantire il corretto funzionamento del mercato, tenendo conto non solo dell'aspetto economico, ma anche dei profili di utilità sociale.

---

[42] Il parametro per determinare l'equo compenso non funziona secondo un normale criterio economico del valore di scambio che avrebbe il contenuto di informazione generato dall'autore, poiché tale valore è creato (o amplificato) dalla stessa piattaforma che lo impiega nella rete (su tale "paradosso del valore" si rinvia a C. MAZZONI, *Creazione e distribuzione del valore nel mercato dei Non-Fungible Token (NFT)*, in *Diritto ed Economia dei Mezzi di Comunicazione*, 2024, 1, p. 77 ss).

[43] A ben vedere una legge in tal senso, sebbene rimasta lettera morta (dovendosene pertanto valutare la portata anche coordinandola con la disciplina dell'equo compenso qui in esame), già esiste: si veda la L. 26 ottobre 2016 n. 198 che ha istituito il "*Fondo unico per il pluralismo e l'innovazione digitale dell'informazione e dell'editoria*", la quale all'art.1, comma 2, espressamente prevede che: "*2. Nel Fondo confluiscono: a) le risorse statali destinate alle diverse forme di sostegno all'editoria quotidiana e periodica, anche digitale, comprese le risorse disponibili del Fondo straordinario per gli interventi di sostegno all'editoria, di cui all'articolo 1, comma 261, della legge 27 dicembre 2013, n. 147; b) le risorse statali destinate all'emittenza radiofonica e televisiva in ambito locale, iscritte nello stato di previsione del Ministero dello sviluppo economico ai sensi dell'articolo 1, comma 162, della legge 28 dicembre 2015, n. 208; c) una quota, fino ad un importo massimo di 100 milioni di euro per l'anno 2016 e 125 milioni di euro per ciascuno degli anni 2017 e 2018, delle eventuali maggiori entrate versate a titolo di canone di abbonamento alla televisione, di cui all'articolo 1, comma 160, primo periodo, lettera b), della legge 28 dicembre 2015, n. 208, come sostituita dall'articolo 10, comma 1, della presente legge; d) le somme derivanti dal gettito annuale di un contributo di solidarietà pari allo 0,1 per cento del reddito complessivo dei seguenti soggetti passivi dell'imposta di cui all'articolo 73 del testo unico delle imposte sui redditi, di cui al decreto del Presidente della Repubblica 22 dicembre 1986, n. 917: 1) concessionari della raccolta pubblicitaria sulla stampa quotidiana e periodica e sui mezzi di comunicazione radiotelevisivi e digitali; 2) società operanti nel settore dell'informazione e della comunicazione che svolgano raccolta pubblicitaria diretta, in tale caso calcolandosi il reddito complessivo con riguardo alla parte proporzionalmente corrispondente, rispetto all'ammontare dei ricavi totali, allo specifico ammontare dei ricavi derivanti da tale attività; 3) altri soggetti che esercitino l'attività di intermediazione nel mercato della pubblicità attraverso la ricerca e l'acquisto, per conto di terzi, di spazi sui mezzi di informazione e di comunicazione, con riferimento a tutti i tipi di piattaforme trasmissive, compresa la rete internet*".

3. Le sanzioni irrogate a Google dall'autorità antitrust francese.

Certamente sarebbe opportuno approfondire il modo in cui il problema è stato affrontato negli altri paesi, verificando, in particolare a livello europeo, come altri stati abbiano attuato (bene o male) la direttiva.

Appare utile ricordare, sia pure solo a livello esemplificativo, che in Canada c'è una proposta di legge[44], così come in California[45], ed anche in Australia già c'è una legge[46] con l'obiettivo di proteggere i contenuti dei giornali e quindi di obbligare le piattaforme digitali a compensare equamente gli editori per riproduzione di notizie (sebbene, come detto, proprio in questi paesi che tentano di legiferare sul punto, Meta ha recentemente chiuso la propria sezione "*News*").

Ma, venendo all'Europa, è utile guardare a quanto è accaduto in Francia, dove - diversamente dall'approccio "autocritico" con cui il TAR del Lazio aveva sospeso la disciplina nazionale sottoponendola al vaglio della Corte di Giustizia Europea - non solo non c'è stato alcun rinvio alla Corte UE, ma sulla legge nazionale francese (legge 2019-775 del 24 luglio 2019 volta a creare un diritto di prossimità a beneficio delle agenzie di stampa e degli editori) è già intervenuta la autorità antitrust con due pronunce consecutive (2020 e 2021)[47] al fine di sanzionare Google per abuso di posizione dominante.

Le misure cautelari e sanzionatorie adottate dall'autorità antitrust francese riguardano le modalità di attuazione da parte di Google della suddetta legge 2019-775, che recepisce nell'ordinamento francese l'articolo 15 della direttiva n. 2019/790 del 17 aprile 2019 sul diritto d'autore e i diritti connessi nel mercato unico digitale, ed è appunto volta a creare le condizioni per una negoziazione equilibrata tra editori, agenzie di stampa e servizi di comunicazione pubblica *on-line*, al fine di ridefinire la condivisione del valore tra questi attori.

---

[44] First Session, Forty-fourth Parliament, 70-71 Elizabeth II, 2021-2022, House of Commons of Canada Chambre, Bill C-18, An Act respecting online communications platforms that make news content available to persons in Canada, First reading April 5, 2022. A questa legge fanno riferimento molti dei critici della normativa italiana, i quali ritengono che il nostro legislatore sembra si sia ispirato a questa "anomala" disciplina.

[45] California Journalism Preservation Act (CJPA), Assembly Bill no. 886, February, 14, 2023, amended in Senate July, 3, 2023.

[46] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021, No. 21, 2021, An Act to amend the Competition and Consumer Act 2010 in relation to digital platforms, and for related purposes.

In attuazione di questo "Codice contrattuale per i news media", varato appena tre anni fa, Facebook e Google avevano sottoscritto una serie di accordi con diversi editori (inclusi la Radio-TV nazionale Abc, Guardian Australia, News Corp Australia, Seven West Media e Nine Entertainment, casa madre dei quotidiani Sydney Morning Herald e The Age di Melbourne) che adesso le piattaforme hanno dichiarato che non intendono rinnovare e tantomeno rinegoziare.

Lo scontro tra Meta e il governo australiano sta assumendo toni di grave contrapposizione, come risulta dalle dichiarazioni del primo ministro Anthony Albanese, il quale ha espresso forte disappunto per la decisione di Meta di chiudere la sezione News definendola "*insostenibile*", preannunciando provvedimenti contro la piattaforma e dichiarando che: "*È disonesto che una compagnia possa profittare di investimenti altrui e non solo investimenti di capitale, ma del lavoro di giornalisti. È un'inadempienza dell'impegno assunto, per la sostenibilità dei mezzi di informazione australiani*" (fonte ANSA, 4 marzo 2024).

[47] La prima: Autorité de la concurrence, Décision n° 20-MC-01 du 9 avril 2020, relative à des demandes de mesures conservatoires présentées par le Syndicat des éditeurs de la presse magazine, l'Alliance de la presse d'information générale e.a. et l'Agence France-Presse; la seconda Autorité de la concurrence, Décision n° 21-D-17 du 12 juillet 2021, relative au respect des injonctions prononcées à l'encontre de Google dans la décision n° 20-MC-01 du 9 avril 2020.

Tuttavia, per ottemperare alla legge, Google aveva deciso unilateralmente che non avrebbe più visualizzato estratti di articoli, fotografie e video dei suoi vari servizi, a meno che gli editori non avessero concesso il permesso di farlo gratuitamente.

Nella decisione sulle misure provvisorie, l'Autorità ha quindi ritenuto che le pratiche in questione potessero costituire un abuso di posizione dominante[48].

Pertanto la Commissione ha emesso sette ingiunzioni nella decisione sulle misure provvisorie al fine di riequilibrare il bilanciamento di potere tra i vari operatori della stampa e le piattaforme digitali e di definire un quadro negoziale imperativo adattato alle circostanze del caso. Le ingiunzioni imponevano a Google - tra gli altri - gli obblighi di avviare trattative in buona fede con gli editori e le agenzie di stampa che lo desiderino (per un periodo di tre mesi dalla data della richiesta dell'editore o dell'agenzia di stampa); di comunicare le informazioni necessarie per una valutazione trasparente della remunerazione prevista dall'articolo L. 218-4 del Codice della Proprietà Intellettuale.

4. La sentenza TAR Lazio 30 ottobre 2023, n. 16069 (Meta c./ AGCM e SIAE).

Anche senza andare all'estero, giova ricordare che lo stesso TAR del Lazio si era pronunciato in maniera opposta, ed a nostro parare assai più convincente per la tutela del mercato digitale, appena un paio di mesi prima, nel caso che ha visto contrapposta la stessa Meta, contro l'AGCM e la SIAE - Società italiana degli autori ed editori[49].

In quest'altro caso, il TAR ha respinto il ricorso intentato da Meta per domandare l'annullamento della delibera con cui l'AGCM le aveva intimato di "*ripristinare immediatamente le trattative - con la Siae - mantenendo un comportamento ispirato ai canoni di buona fede e correttezza, provvedendo altresì a fornire tutte le sole informazioni necessarie per ristabilire un equilibrio nell'intero rapporto commerciale e ripristinare tempestivamente, in modo pieno, la disponibilità dei contenuti musicali tutelati da Siae sulle proprietà di Meta per tutto il periodo necessario alla conclusione del negoziazioni*".

In questa vicenda, che aveva visto il pubblico dei fruitori dei *social network* di Meta (i.e. *Facebook*) privato dei contenuti musicali a causa del mancato accordo di Meta con la SIAE per l'equo compenso del diritto d'autore spettante per la riproduzione dei brani, il TAR ha tenuto conto della pluralità degli interessi sottesi: ha infatti mostrato una significativa attenzione al quadro d'insieme, che gli ha consentito di tenere conto che il *social network* della piattaforma dominante nel nuovo mercato digitale[50] è uno spazio in cui necessariamente gli autori dei contenuti e i fruitori debbono essere garantiti, nel pubblico interesse.

---

[48] Cfr. nota 50.

[49] TAR Lazio, 30.10.2023, n. 16069/2023 Reg.Prov.Coll., n. 08974/2023 Reg.Ric., n. 08975/2023 Reg.Ric.

[50] La sentenza ha costituito l'occasione per analizzare, attraverso una interessante ed approfondita indagine, come debbano essere considerati i requisiti adoperati dall'art. 9 l.192/1998, evitando un approccio semplicistico e dovendo tener conto di tutte le circostanze esterne che derivano dal contesto esterno: il rinvio è a C. MEO, *Dipendenza economica tra società di gestione collettiva e social network: spunti alla luce del caso Meta c. SIAE*, in corso di pubblicazione su AIDA, Annali Italiani del Diritto d'Autore, 2023. Pur essendosi osservato, in senso dubitativamente critico rispetto a quanto ritenuto da questa decisione, che, a ben

Di talché non si è consentito alla piattaforma di sottrarsi egoisticamente alla trattativa e di escludere quindi i contenuti musicali protetti dal diritto d'autore, che pertanto ha dovuto necessariamente acquisire, concludendo la negoziazione.

Qui il TAR sceglie di proteggere la posizione non solo della SIAE ma anche dell'AGCM: ciò a differenza di quanto accaduto alla AGCOM nell'altra decisione qui in esame, in cui il TAR ha - per converso - reputato contrario alla libera concorrenza il meccanismo dell'equo compenso (peraltro richiamando a sostegno un parere conforme della stessa AGCM).

A pag.11 di questa sentenza - tenendo bene in considerazione lo "*strapotere delle piattaforme*" (pag. 13) e il loro ruolo "*infungibile*" per gli autori e per il pubblico dei fruitori - si legge che "*9.9. A fronte di tali numeri, l'eventuale impedimento all'accesso alla piattaforma costituisce un vulnus gravissimo per gli artisti: d'altronde, come efficacemente rappresentato dalla difesa di Siae (che cita all'uopo letteratura specialistica), la «scoperta» del contenuto musicale avviene tendenzialmente sui social network, costituendo ciò la premessa della successiva «fruizione», vuoi sulle piattaforme musicali dedicate, vuoi attraverso i canali tradizionali. Appare manifesto, quindi, il ruolo fondamentale delle piattaforme della società ricorrente nella diffusione dei contenuti musicali. 9.10. Viepiù, va rilevato come la possibilità che i prodotti tutelati da Siae possano essere fruiti digitalmente in altro modo non costituisce alternativa soddisfacente, atteso che la chiusura dei canali digitali di Meta non appare surrogabile con altri strumenti: semplificando, la circostanza che Facebook o Instagram abbiano dei concorrenti nel mercato dei social network (in particolare Tik Tok) non implica automaticamente che il servizio offerto da quest'ultima impresa possa considerarsi un'alternativa soddisfacente. Ogni social network, infatti, si caratterizza per delle peculiarità differenziali che lo rendono spesso infungibile per il pubblico. Ciò è tanto più vero nel caso all'odierno esame dove una delle reti sociali di Meta (ossia Facebook, quella notoriamente più «generalista») da sola gestisce un numero di account quasi doppio rispetto a quelli del principale concorrente*".

5. Autodisciplina e co-regolazione: un'opportunità di efficienza delle fonti normative del mercato digitale necessaria e conveniente per le stesse piattaforme.

In conclusione, pur prescindendo dai contenuti tecnici del regolamento sull' equo compenso, seppure migliorabili, in ogni caso non sarebbe stato opportuno reprimere e stroncare sul nascere la sperimentazione in corso, che – se correttamente condotta – può portare a risultati utili, nell'ottica della leale cooperazione tra tutti i protagonisti, mediante - appunto - la "*co-regolazione*", che scaturisce dal principio di sussidiarietà di cui all'art. 118 Cost.

---

vedere, nel caso di specie potrebbero difettare i presupposti per integrare la fattispecie dell'abuso della posizione dominante, ciononostante la soluzione ben potrebbe essere opposta ove rilevi il diritto all'informazione e comunque sia, per quanto qui interessa, anche se non ricorresse la fattispecie dell'abuso, in ogni caso resta la necessità di adottare adeguate strategie di regolazione che garantiscano la tutela degli interessi sottesi, anche di rilevanza costituzionale, che non possono essere abbandonati alle regole del mercato.

L'auspicio è che la Corte di giustizia UE, nel valutare la compatibilità del regolamento sull'equo compenso con la normativa comunitaria, sappia valutare bene l'importanza del caso sia per l'implementazione della tecnica normativa della *co-regolazione*, sia per la sopravvivenza del pluralismo dell'informazione e dunque per la tutela dei diritti fondamentali.

Dietro questo episodio c'è di più.

Esso deve essere adeguatamente valutato e interpretato non soltanto nei limiti del regolamento sull'equo compenso, in quanto (come si preannuncia anche per il nuovo fronte della contrapposizione estesa al ROC), traspare evidentemente più che una "*insofferenza a qualsiasi forma di regola*" da parte delle piattaforme digitali, o quantomeno di alcune di esse, così come è stato notato da un commissario della stessa AGCOM[51].

Non è questo l'approccio giusto, ma, giova ribadire, occorre una consapevolezza culturale di tutti gli operatori del sistema (autorità, magistratura, dottrina) che queste novità tecnologiche richiedono nuove forme di regolazione e di composizione dei contrapposti interessi.

Ciò innanzitutto nell'interesse generale del mercato e a tutela dei diritti fondamentali del pubblico della rete, ma anche nell'interesse (privato ed individuale) di tutti i protagonisti. Anche dei più forti. E dunque delle piattaforme digitali.

Si affacciano pertanto alcuni importanti interrogativi, dovendosi presumere che, ovviamente, Mark Zuckerberg e Jeff Bezos siano correttamente informati che - nel piccolo e complesso mercato europeo - le sedi italiane delle loro multinazionali stanno promuovendo questi ricorsi[52]: siamo certi che ci sia piena consapevolezza delle future conseguenze di questa strategia politica adottata da Meta e da Amazon? La logica del conflitto con ogni forma di regolazione degli Stati si pone ugualmente per tutti i paesi o solo in misura diversa per alcuni? Sarà condivisa anche con le altre piattaforme (*over the top*) che sembrano avere manifestato maggiore disponibilità al dialogo (come Apple e Google)?

Se volontà delle piattaforme è quella di respingere ogni forma di cooperazione con gli Stati, nel tentativo di stabilire regole condivise, allora anche la politica degli Stati in futuro finirà per dover intraprendere strade diverse, non più in una logica di cooperazione, bensì - purtroppo - di sola contrapposizione.

E questo - nel lungo termine - non sarebbe un buon risultato nemmeno per le piattaforme, nonostante l'attuale debolezza degli Stati, incapaci di dettare regole nel mercato rispetto allo strapotere economico delle piattaforme stesse.

[51] https://www.huffingtonpost.it/blog/2024/02/22/news/difendere_il_regolamento_agcom_vuol_dire_difendere_la_libera_informazione-15196483/.

[52] Tuttavia il problema si pone in termini analoghi anche in altri paesi, come dimostra la scelta di Meta di chiudere la sezione "*News*" in Regno Unito, Germania, Francia, Canada e Australia, come più volte richiamato.

Caso R, 'Diritto, politica ed economia dell'innovazione tecnologica: 1940, 1980, 2020' (2023) 2 EJPLT, 56 - 61.
DOI: https://doi.org/10.57230/EJPLT232RC

EJPLT
ISSN 2704-8012



Diritto, politica ed economia dell'innovazione tecnologica: 1940, 1980, 2020*

Law, policy and economics of technological innovation: 1940, 1980, 2020

ROBERTO CASO
Professore Ordinario di Diritto Privato Comparato
Università degli studi di Trento

Abstract

Nella politica di ricerca e innovazione (R&I) dell'Unione Europea, da un lato si moltiplicano le azioni di promozione dell'Open Science (OS) delle università, dall'altro si estendono i diritti di proprietà intellettuale e se ne incoraggia l'uso e il trasferimento a privati nelle stesse istituzioni accademiche.
In un ecosistema di R&I dominato dal capitalismo del monopolio intellettuale, la promozione dell'OS rischia di essere, nel migliore dei casi, inefficace o poco efficace e, nel peggiore, uno strumento per rafforzare i monopoli stessi.

In European Union Research & Innovation (R&I) policy, on the one hand, actions promoting universities' Open Science (OS) are growing, and on the other hand, Intellectual Property Rights are being extended and their use and transfer to private individuals is being encouraged in academic institutions themselves.
In a R&I ecosystem dominated by intellectual monopoly capitalism, the promotion of OS runs the risk of being, at best, ineffective or limitedly effective and, at worst, a tool to strengthen the monopolies themselves.

*Questo articolo è stato presentato alla conferenza internazionale "Il diritto dell'innovazione tecnologica. Jam Session internazionale tra giuristi", 8-9 marzo 2023, Fondazione Einaudi, Roma.
Comitato scientifico: Vincenzo Ricciuto (Univ. Tor Vergata di Roma), Lucilla Gatt (Univ. Suor Orsola Benincasa di Napoli), Carla Solinas (Univ. Tor Vergata di Roma), Mariló Gramunt Fombuena (Universitat de Barcelona).

© The author(s) 2023, 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: Unione Europea; Proprietà intellettuale; Scienza aperta.

Summary: 1. Introduzione. – 2. Law and Political Economy. – 3. L'approccio legislativo europeo al rapporto tra università, innovazione tecnologica e proprietà intellettuale. – 4. La scienza aperta nell'era capitalismo dei monopoli intellettuali. 5. Conclusioni.

Introduzione.[1]

Grazie al prof. Vincenzo Ricciuto per avermi invitato a dialogare con autorevoli colleghe e colleghi nell'ambito di questa jam session sul diritto dell'innovazione tecnologica.

Proverò ad occuparmi di diritto, politica ed economia nel rapporto tra università, proprietà intellettuale e innovazione tecnologica.

In questa mia brevissima (e non so quanto felliniana) "prova d'orchestra" offrirò uno sguardo da realista e comparatista al tema in discussione.

Farò riferimento a tre date simboliche di cui si capirà meglio il significato alla fine del mio intervento: 1940, 1980, 2020. Il nesso con la prima data simbolica, l'anno 1940, sarà svelato solo alla fine.

Vincenzo Ricciuto ha gentilmente offerto una lista di domande per dare inizio alla musica.

Ne ho scelte due:

a) Quali dovrebbero essere i tratti caratteristici e specifici della metodologia della ricerca giuridica nel campo dell'innovazione tecnologica?

b) Quali sono i pregi e le mancanze del modo di legiferare dell'UE in tema di nuove tecnologie?

2. Law and Political Economy.

Credo che uno dei meriti della comparazione giuridica italiana sia stato di aver contribuito ad alimentare un approccio critico al diritto. La comparazione va realisticamente oltre l'approccio formalista al diritto positivo per indagare storicamente l'evoluzione dei sistemi giuridici. E va oltre il diritto positivo di un Paese non solo mettendo a confronto sincronico i sistemi giuridici contemporanei ma anche dialogando con altri saperi: la linguistica, l'antropologia, l'economia, l'informatica, le scienze biomediche, l'arte, la letteratura ecc.

Per comprendere pregi e mancanze del modo di legiferare dell'UE serve una buona metodologia d'indagine critica e interdisciplinare. Il mio suggerimento è che questa metodologia potrebbe ispirarsi ad un nuovo movimento di idee che passa sotto il nome "Law and Political Economy" e vede tra i suoi promotori

[1] L'immagine sulla prima pagina raffigura la Testa di Platone, copia romana. L'originale è stato esposto nell'Accademia dopo la morte del filosofo (348/347 AC). https://it.wikipedia.org/wiki/Dialoghi_platonici#/media/File:Head_Platon_Glyptothek_Munich_548.jpg

Amy Kapczynski di Yale[2]. La premessa dalla quale parte il movimento è che politica ed economia non possono essere separate e che entrambe sono strettamente intrecciate con il diritto. In un'epoca segnata dal cambiamento climatico, dalle guerre, nonché dalle diseguaglianze enormi e crescenti che mettono a rischio i sistemi democratici, occorre indagare i fenomeni come l'innovazione tecnologica tenendo congiuntamente presenti le tre dimensioni della politica, dell'economia e del diritto.

3. L'approccio legislativo europeo al rapporto tra università, innovazione tecnologica e proprietà intellettuale.

Nella prospettiva di Law and Political Economy, l'approccio legislativo europeo al rapporto tra università, innovazione tecnologica e proprietà intellettuale è stato pesantemente influenzato da quello statunitense per via diretta o per via indiretta, attraverso trattati internazionali, sui quali la voce degli USA ha contato molto.

Due sono gli aspetti notevoli della politica e della legislazione europea sui quali vorrei provare ad attirare l'attenzione.

1) L'assunto che l'estensione della proprietà intellettuale (nuovi diritti di proprietà intellettuale e rafforzamento delle esclusive) condurrebbe a maggiore innovazione. Si tratta di una sorta di equazione: più proprietà intellettuale equivale a più innovazione tecnologica.

2) Una visione strumentale dell'università finalizzata a garantire un flusso di diritti di proprietà intellettuale dalla ricerca di base (appannaggio delle istituzioni accademiche) alla ricerca applicata (appannaggio delle imprese, e in particolare delle start-up). Si tratta dell'idea alla base del Bayh-Dole Act statunitense del 1980[3]. 1980, ecco la seconda data simbolica!

Gli europei si sono, talora, dimostrati più realisti del re. Cioè più estremisti degli americani. Per esempio, quando nel 1996 hanno introdotto il diritto sui generis sulle banche dati, ritenendo che ciò avrebbe dato un vantaggio competitivo alle imprese europee[4]. Assunto poi dimostratosi disastrosamente infondato. Nell'ultima legislazione sui dati (Open Data Directive, Data Governance Act, Data Act) l'UE ha tentato di arginare il diritto sui generis. Resta il fatto, però, che si è scelto di tenere in vita un diritto di esclusiva il cui effetto incentivante è – a detta della stessa Commissione UE – indimostrato.

---

[2] A. KAPCZYNSKI ET AL., *New Law and Political Economy Project Launched*, 29.04.2019. Consultabile al sito: https://law.yale.edu/yls-today/news/new-law-and-political-economy-project-launched; J.S. BRITTON-PURDY, D.S. GREWAL, A. KAPCZYNSKI, AMY, K.S. RAHMAN, *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis* (March 2, 2020), in *Yale Law Journal*, Columbia Public Law Research Paper No. 14-657. Consultabile al sito: https://ssrn.com/abstract=3547312

[3] D. TRAFICONTE, *Property and Power on the Endless Frontier* (August 9, 2021). Consultabile al sito: https://ssrn.com/abstract=3901914

[4] C. SGANGA, *Ventisei anni di direttiva database alla prova della nuova strategia europea per i dati: evoluzioni giurisprudenziali e percorsi di riforma*, in *Diritto dell'informazione e dell'informatica*, 2022, 651-704.

4. La scienza aperta nell'era del capitalismo dei monopoli intellettuali.

Una tesi, supportata da un'ampia letteratura scientifica, sostiene che l'estensione della proprietà intellettuale e la visione strumentale dell'università hanno nutrito il capitalismo dei monopoli intellettuali deprimendo l'innovazione, accrescendo la disuguaglianza e mettendo a rischio la democrazia[5]. Il quadro è ulteriormente peggiorato quando alla proprietà intellettuale si è aggiunta la pseudo-proprietà intellettuale cioè quel complesso di forme anomale di esclusiva che vanno oltre i limiti tradizionali della proprietà intellettuale e si fondano soprattutto sul controllo contrattuale e di fatto (cioè assistito dalla forza bruta della tecnologia) di dati e informazioni.

In un modello stilizzato e ideale di innovazione tecnologica di un sistema capitalistico di libero mercato ci sono, a monte, il settore pubblico e le università che creano ricerca di base attenendosi ai principi della scienza aperta e, a valle, un mercato concorrenziale che produce ricerca applicata e si serve di una proprietà intellettuale limitata per commercializzare le nuove tecnologie. La concorrenzialità del mercato spinge verso il basso il prezzo della tecnologia, in modo da garantire attraverso contratti o mediante meccanismi redistributivi (ad es. sovvenzioni pubbliche) l'accesso all'innovazione.

Questa idealizzazione è distante anni luce dalla realtà attuale per diversi ordini di ragione.

a) Le università non sono più entità nettamente distinte dalle aziende, perché sono organizzate secondo logiche aziendali, anche sul piano della valutazione. Si tratta di una questione giuridica (architettura istituzionale e norme sulla valutazione), ma anche di etica e mentalità.

b) Le prassi accademiche e l'etica della scienza aperta sono state progressivamente erose dal crescente ricorso da parte dei ricercatori alla proprietà intellettuale[6]. Tale uso estensivo dei diritti esclusiva è il frutto di incentivi sia economici sia valutativi (si pensi, al fatto che sul piano della valutazione della ricerca accademica i brevetti sono, almeno in Italia, considerati equivalenti alle pubblicazioni scientifiche). L'uso della proprietà intellettuale innesca conflitti insanabili tra l'interesse a perseguire il progresso della conoscenza e l'interesse al profitto. Per rendersene conto è sufficiente leggere le ragioni che hanno spinto l'Istituto Mario Negri a rinunciare ai brevetti[7].

---

[5] U. PAGANO, *The Crisis of Intellectual Monopoly Capitalism* (November 13, 2014), in *Cambridge Journal of Economics* V. 38, 1409-1431. Consultabile al sito: https://ssrn.com/abstract=2537972. U. PAGANO, *Il capitalismo dei monopoli intellettuali*, in *Menabò Eticaeconomia*, 14 dicembre 2021. Consultabile al sito: https://www.eticaeconomia.it. M. FLORIO, *La privatizzazione della conoscenza*, Bari-Roma, 2021.

[6] Già nel 1988 Robert Merton poteva affermare, 623: "Current renewed tendencies toward secrecy, and not alone in what Henry Etzkowitz has described as 'entre-preneurial science', […] will, if extended and prolonged, introduce major change in the institutional and cognitive workings of science" (R.K. MERTON, *The Matthew Effect in Science, II: Cumulative Advantage and the Symbolism of Intellectual Property,* in *Isis*, 79(4), 1988, 606-623).

[7] ISTITUTO DI RICERCHE FARMACOLOGICHE MARIO NEGRI IRCCS, *Perché non brevettiamo le nostre ricerche*. Consultabile al sito: https://www.marionegri.it/non-brevettiamo. "Mantenere un'istituzione di ricerca in equilibrio costante fra la necessità di trovare risorse per fare ricerca, senza rinunciare alla propria libertà, alla dignità, allo spirito critico, è impresa difficile e complicata. Soprattutto in Italia, dove i fondi pubblici sono scarsi e male utilizzati. È quindi opportuno che l'opinione pubblica impari a distinguere fra chi cura interessi personali e chi si occupa di interessi della comunità, per non far mancare il suo sostegno a questi ultimi". S. GARATTINI, *Brevettare la salute? Una medicina senza mercato*, Bologna, 2022, 125.

c) I grandi monopoli intellettuali non devono necessariamente aspettare che il settore pubblico e le università decidano di trasferire la conoscenza, perché sono in grado di appropriarsene direttamente. Si pensi al crescente dominio delle Big Tech nel campo delle infrastrutture accademiche, dominio che si esprime non solo nell'appropriazione di dati della ricerca scientifica (ora finalizzata anche all'addestramento dell'intelligenza artificiale), ma anche di dati personali degli scienziati (è noto che nell'ambito della ricerca scientifica opera diffusamente il capitalismo della sorveglianza)[8]. Si pensi altresì alla cattura culturale tramite il ricco finanziamento di progetti i cui risultati sono orientati agli interessi dei finanziatori privati (i monopoli intellettuali)[9].

d) La geopolitica interferisce nelle dinamiche di chiusura e apertura dell'innovazione[10]. In tempi di guerre e crescente tensione tra diverse potenze, la chiusura della conoscenza scientifica viene usata come strumento bellico.

Quanto finora rilevato potrebbe apparire in stridente contraddizione con il fatto che le politiche dell'UE in materia di rapporto tra università, proprietà intellettuale e innovazione tecnologica hanno negli ultimi venti anni riguardato anche la promozione dell'Open Science. È innegabile, infatti, che l'UE abbia sviluppato un'ampia, articolata e – per molti versi – meritoria politica di promozione della scienza aperta.

Tuttavia, la strategia di difesa e rafforzamento della proprietà intellettuale è rimasta sostanzialmente invariata. Come è rimasta invariata la concezione del rapporto tra università, proprietà intellettuale e innovazione tecnologica. Basti pensare a quanto accaduto durante la pandemia di Covid-19 a proposito della proprietà intellettuale sui vaccini. E siamo giunti alla terza data simbolica: il 2020.

L'UE è stata tra i più strenui oppositori della proposta di India, Sudafrica e molti altri Paesi di sospendere i TRIPS al fine di facilitare la produzione di dispositivi medici, farmaci e vaccini. Nello stesso tempo non è stata in grado di sviluppare, produrre e distribuire vaccini interamente europei. Si è dovuta, in gran parte, affidare a imprese non europee come Pfizer e Moderna.

5. Conclusioni

In un ecosistema dell'innovazione tecnologica dominato dal capitalismo dei monopoli intellettuali, la promozione della scienza aperta rischia di essere, nel migliore dei casi, inefficace e, nel peggiore, uno strumento per rafforzare gli stessi monopoli.

---

[8] K. MAEX, *Protect independent and public knowledge*, Jan 8, 2021. Consultabile al sito: https://uvaauas.figshare.com/: "What applies to the future of democracy applies equally to the future of universities and of independent education and research as vital building blocks for the organisation of knowledge. We cannot simply leave the future of knowledge to the corporate boardrooms"; M.C. PIEVATOLO, *I custodi del sapere*, in *Bollettino Telematico di Filosofia Politica*, 31 maggio 2021. Consultabile al sito: https://btfp.sp.unipi.it/it/2021/05/i-custodi-del-sapere/

[9] D. TAFANI, *L'«etica» come specchietto per le allodole. Sistemi di intelligenza artificiale e violazioni dei diritti*, in *Bollettino telematico di filosofia politica*, 2023. Consultabile al sito: https://commentbfp.sp.unipi.it/letica-come-specchietto- per-le-allodole/

[10] R. CASO, *Pandemia e vaccini: scienza aperta o proprietà intellettuale?*, 23 maggio 2021, Trento LawTech Research Paper series nr. 44, in *Rivista critica del diritto privato*, 39(2), 2021, 267-286. Consultabile al sito: https://zenodo.org/records/4783183#.YKubWpMzY6A

Per promuovere la scienza aperta intesa come scienza pubblica e democratica occorrerebbe procedere seriamente verso la demolizione dei monopoli intellettuali, a cominciare da una seria e organica riforma della proprietà intellettuale. Ma questo sembra un compito estraneo all'agenda politica di questi e, con tutta probabilità, dei prossimi organi decisionali dell'UE.

La scienza aperta è parte integrante della liberà accademica e del dialogo cosmopolita che aiuta la cooperazione e la pace[11]. Insomma, è un insieme di valori e ideali che sembra condannato alla marginalità. A meno che le nuove generazioni dentro e fuori dall'Europa non siano capaci di costruire un futuro migliore del presente che abbiamo consegnato loro.

Torniamo ora alla prima data simbolica: il 1940. Luigi Einaudi, al cui nome e alla cui memoria è intitolata la Fondazione sede di questo convegno, poteva scrivere nell'anno in cui l'Italia entrò nella Seconda guerra mondiale:

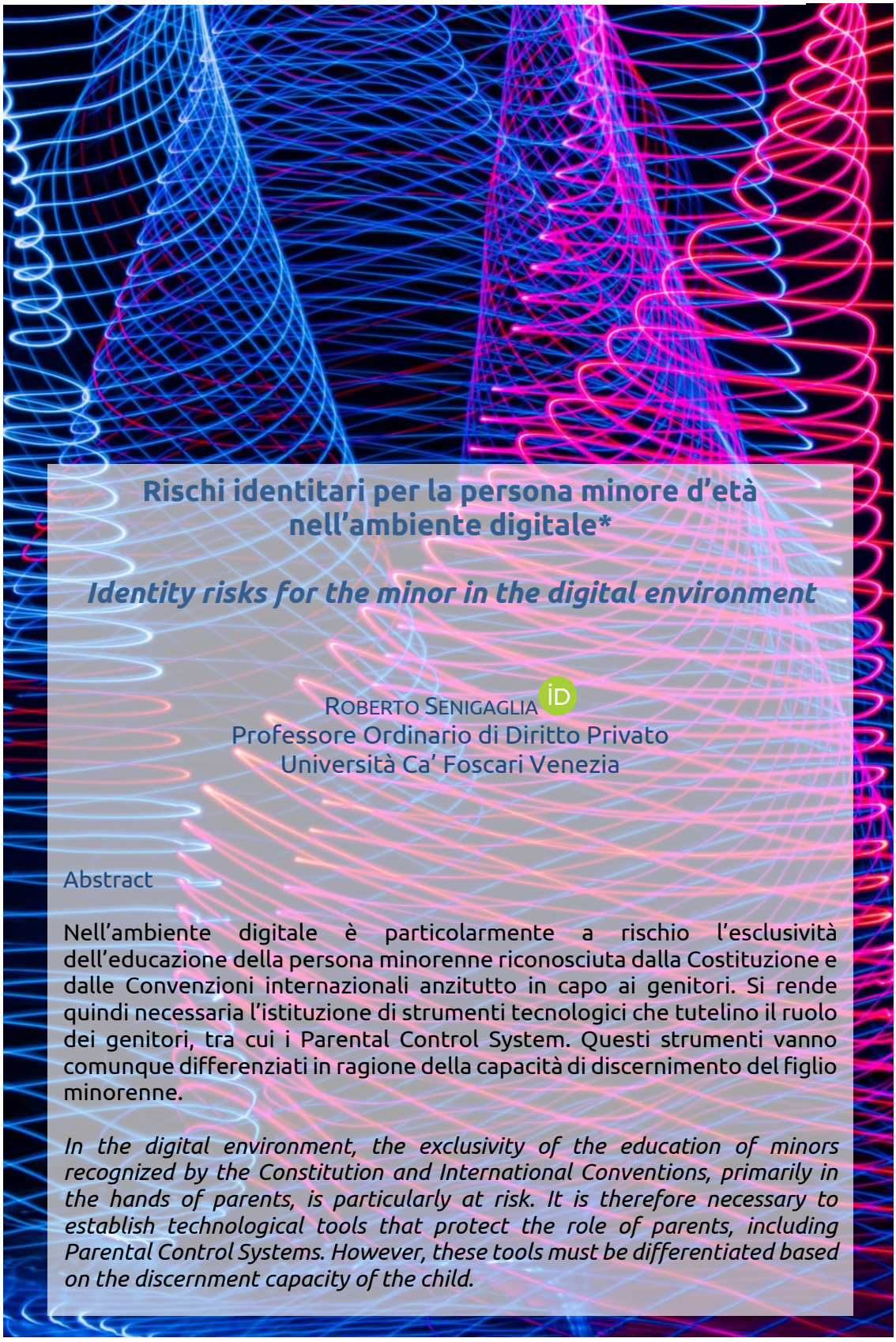
"Si è più scettici intorno alla probabilità che la garanzia concessa agli scrittori ed inventori dello sfruttamento esclusivo temporaneo del libro e dell'invenzione conduca al desiderato scopo. Si teme l'incoraggiamento inutile delle cattive lettere in materia di proprietà letteraria e il monopolio dei grossi potenti accaparratori e fabbricanti di invenzioni in materia di proprietà industriale. […] I pericoli proprii del sistema odierno sono così gravi, particolarmente per la proprietà industriale, che una revisione dei principii della legislazione oggi invalsa in quasi tutti i paesi appare urgente"[12].

[11] AISA (MARIA CHIARA PIEVATOLO), *Scienza aperta e pace*, 05.11.2022. Consultabile al sito: https://aisa.sp.unipi.it/scienza-aperta-e-pace/

[12] L. EINAUDI, *Rileggendo Ferrara – a proposito di critiche recenti alla proprietà letteraria ed industriale*, in *Rivista di storia economica*, V, n. 4, dicembre 1940, 217-256. Consultabile al sito: https://www.luigieinaudi.it/doc/rileggendo-ferrara-a-proposito-di-critiche-recenti-alla-proprieta-letteraria-ed-industriale/

Senigaglia R, 'Rischi identitari per la persona minore di età nell'ambiente digitale' (2023) 2 EJPLT, 62 - 70.
DOI: https://doi.org/10.57230/EJPLT232RS

EJPLT
ISSN 2704-8012



Rischi identitari per la persona minore d'età nell'ambiente digitale*

Identity risks for the minor in the digital environment

ROBERTO SENIGAGLIA
Professore Ordinario di Diritto Privato
Università Ca' Foscari Venezia

Abstract

Nell'ambiente digitale è particolarmente a rischio l'esclusività dell'educazione della persona minorenne riconosciuta dalla Costituzione e dalle Convenzioni internazionali anzitutto in capo ai genitori. Si rende quindi necessaria l'istituzione di strumenti tecnologici che tutelino il ruolo dei genitori, tra cui i Parental Control System. Questi strumenti vanno comunque differenziati in ragione della capacità di discernimento del figlio minorenne.

In the digital environment, the exclusivity of the education of minors recognized by the Constitution and International Conventions, primarily in the hands of parents, is particularly at risk. It is therefore necessary to establish technological tools that protect the role of parents, including Parental Control Systems. However, these tools must be differentiated based on the discernment capacity of the child.

*Questo articolo è stato presentato alla conferenza internazionale "Il diritto dell'innovazione tecnologica. Jam Session internazionale tra giuristi", 8-9 marzo 2023, Fondazione Einaudi, Roma.
Comitato scientifico: Vincenzo Ricciuto (Univ. Tor Vergata di Roma), Lucilla Gatt (Univ. Suor Orsola Benincasa di Napoli), Carla Solinas (Univ. Tor Vergata di Roma), Mariló Gramunt Fombuena (Universitat de Barcelona).

© The author(s) 2023, 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: Affiliation relationship; duty to educate children; cyberspace; Parental Control System.

Summary: Introduzione: La questione identitaria. – 1. Il fattore eversivo dello statuto educativo del minorenne in formazione. – 2. Internet Free Speech e ruolo educativo dei genitori: il Parental Control System. – 3. Necessità di differenziare le forme di controllo parentale nell'ambito della minore età.

Introduzione: La questione identitaria.

La questione problematica su cui intendiamo soffermarci concerne l'impatto dell'esperienza [1] digitale sull'identità del minore, riguardante, in particolar modo, la sua biografia (e non tanto l'anagrafe e il profilo genetico)[2], e sulle capacità di risposta normativa. L'originalità dell'articolazione del problema discende dall'implicazione, nelle relazioni telematiche, della cifra ermeneutica dell'altrove, così come recentemente pensata, del fatto che «il server è altrove, rispetto all'artefatto tecnologico che stiamo usando, così come sono altrove le possibili persone con cui possiamo interagire ed è sempre altrove la fonte dei contenuti di cui fruiamo»[3].

Un *altrove* che, diversamente da come possa essere affrontato con riferimento alla persona adulta, conosce profili di maggiore complessità quando entra in contatto con una persona minorenne. Difatti, mentre per l'adulto la questione si traduce, principalmente, nell'apprestare gli strumenti più idonei a tutelare il diritto a non vedere pregiudicata (finanche sottratta), in vario modo, la propria identità personale; per il minorenne il problema può riguardare, anche in via esclusiva, la salvaguardia dell'interesse a *formarsi* una propria identità.

Segnatamente, con riguardo alla "stagione" della minore età, l'identità personale [4], si pone in una duplice direzione funzionale: *costruttiva* e *conservativa* della personalità.

Ebbene, nell'esperienza digitale del minore, di queste due direzioni funzionali dell'identità personale, risulta di maggiore interesse (se non altro perché meno indagata) quella *costruttiva*, concernente cioè il momento formativo della personalità morale[5].

Il profilo giuridicamente sensibile è che l'irrompere del digitale nella vita del minore, sin dalla prima infanzia, assume, da subito, carattere pervasivo della

[1] Riferita non soltanto a ciò che ci capita, ma anche a ciò che facciamo di quello che ci capita; in proposito, v. A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, Milano-Udine, 2023, p. 41, il quale riprende, in questi termini, l'espressione di Huxley.

[2] Sulle diverse dimensioni dell'identità si rinvia a P. Zatti, *Dimensioni e aspetti dell'identità nel diritto privato attuale*, in *L'identità nell'orizzonte del diritto privato*, in *Nuova giur. civ. comm.*, Supplemento al fascicolo 4/2007, p. 1 ss.; S. Rodotà, *Quattro paradigmi per l'identità*, ivi, p. 21 ss.; V. Scalisi, *L'ermeneutica della dignità*, Milano, 2018, *passim*; A. La Spina, *Complessità e identità personale*, Napoli, 2022, *passim*.

[3] A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., p. 47.

[4] Da intendersi come diritto ad «essere uguale solo a se stesso e diverso da tutti gli altri», così F. Giardina, *Interesse del minore: gli aspetti identitari*, in *Nuova giur. civ. comm.*, 2016, II, p. 159.

[5] A. Nicolussi, voce *Autonomia privata e diritti della personalità*, in *Enc. dir.*, Annali, IV, Milano 2011, p. 138; G. Resta, *Dignità, persone e mercati*, Torino, 2014, p. 103.

persona[6]: non soltanto a seguito dell'utilizzo diretto degli artefatti tecnologici, ma pure per effetto della circolazione (e, dunque, del trattamento *ex* art. 4, par. 1, n. 2), Reg. (UE) 2016/679) dei suoi dati personali nella rete, innescata dai genitori, da altri familiari o da terzi soggetti[7], ivi inclusi gli operatori del *web*. Tutto ciò con il rischio che i dati personali, spesso acquisiti nel mancato rispetto delle coordinate fissate dal GDPR tra protezione e circolazione[8], finiscano in qualche trama della rete che "restituisca" al minore pezzi mancanti della sua identità, *eteroimposti* dalla tirannia degli algoritmi[9] e, quindi, sottratti alla formazione *naturale* della sua personalità morale, rispondente alle sue capacità, aspirazioni e inclinazioni naturali.

1. Il fattore eversivo dello statuto educativo del minorenne in formazione.

È in questa dinamica che si insinua il fattore eversivo dello statuto educativo del minorenne *in formazione*, vale a dire l'*eteroimposizione* anziché l'*eterodeterminazione* della sua identità personale[10].

Difatti, con riguardo al "piccolo minore", sprovvisto della capacità di discernimento, è essenzialmente l'educazione che porta a compimento l'opera di edificazione della personalità del figlio[11]. Una funzione che già la Costituzione assegna anzitutto ai genitori e, soltanto in caso di incapacità di

---

[6] Sul tema V. Corriero, Privacy *del minore e potestà dei genitori*, in *Rass. dir. civ.*, 2004; A. Thiene, *L'inconsistente tutela dei minori nel mondo digitale*, in *Studium iuris*, 2012, p. 528 ss.; C. Camardi, *Minori e* privacy *nel contesto delle relazioni familiari*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pisa, 2019, p. 122; V. Andreoli, *La famiglia digitale. Come la tecnologia ci sta cambiando*, Milano, 2021, *passim*; R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, in *Pers. merc.*, 2021, p. 518 ss.; E. Battelli, *Il trattamento dei dati nel prisma della tutela della persona minore di età*, in *Dir. inf.*, 2022, p. 267.

[7] Relativamente alla pubblicazione di immagini del minore da parte dell'ex compagna del padre v. Trib. Bari, 7 novembre 2019, in *Dir. internet*, 2020, p. 87 ss., con commento di Maggi, *Consenso e tutela del diritto all'immagine del minorenne: tra diritto della personalità e protezione dei dati dei minori*.

[8] Su questi aspetti si rinvia ad Aa.Vv., *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, opera diretta da G. Finocchiaro, Bologna 2017; V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; A. De Franceschi, R. Schulze, *Digital revolution-new challenges for law. Data protection, artificial intelligence, smart products, blockchain technology and virtual currencies*, Baden-Baden, 2019, p. 75 ss.; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019; C.J. Hoofnagle, B. van der Sloot, F. Zuiderveen Borgesius, *The European Union general data protection regulation: what it is and what it means*, in *Information & Communications Technology Law*, 2019, p. 65 ss.;L. Bozzi, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Eur. dir. priv.*, 2020, p. 253; R. Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2020, p. 75 ss.; V. Ricciuto, *L'equivoco della privacy. Persona vs. dato personale*, Napoli, 2022, *passim*; B. Parenzo, *Sull'importanza del dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali gratuiti*, in *Dir. fam.*, 2021, p. 1457 ss.; A. Bernes, *Enhancing Transparency of Data Processing and Data Subject's Rights Through Technical Tools: The PIMS and PDS Solution*, in R. Senigaglia, C. Irti, A. Bernes, *Privacy and Data Protection in Software Services*, Singapore, 2022, p. 197 ss.

[9] Si rinvia a T.Z. Zarsky, *"Mine your own business!": making the case for the implications of the data mining of personal information in the forum of public opinion*, in *Yale Journal of Law and Technology*, 2003, p. 1 ss.; F. Pasquale, *The Black Box Society. The secret algorithms that control money and information*, Cambridge, Massachusetts, London, 2015; S. Rodotà, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014, p. 38 ss.; L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, p. 72 ss.; S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma*,* 2019, *passim.*

[10] Su questi diversi profili si rinvia a P. Zatti, *Dimensioni e aspetti dell'identità nel diritto privato attuale*, cit., p. 4 ss.

[11] Cfr. A. Thiene, *Gioventù bruciata online: quale responsabilità per i genitori?*, in A. Annoni e A. Thiene (a cura di), *Minori e privacy. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Napoli, 2019, p. 41 ss.

questi, demanda alla legge il compito di individuare delle figure vicarie (art. 30, commi 1 e 2); comunque, essa deve essere assolta in modo *naturale*, ovvero non secondo schemi astratti, definiti una volta per tutte, ma cogliendo dalla narrazione dell'*essere* del figlio gli spunti di metodo della pedagogia dell'*apparire*[12].

Nell'era pre-digitale, questa funzione *costruttiva* dell'identità personale del figlio era pacificamente prerogativa *esclusiva* dei genitori. Esclusività garantita anche nel caso in cui intervengano elementi di alterità; altri soggetti, cioè, partecipino all'educazione del figlio, cooperando alla formazione della sua biografia. In queste situazioni, invero, i genitori versano nella condizione materiale di poter affermare la loro "esclusiva", giacché l'esposizione antropologica del figlio riguarda comunque *altri* (identificati o identificabili), permanendo, quindi, nella loro sfera di controllo.

Questa *esclusività* rischia, invece, di essere scardinata nel momento in cui il figlio accede alla rete[13]. Il *web*, per mezzo del meccanismo, talvolta spasmodico e inconsapevole,[14] di *input* (composti per lo più da dati personali del minore) e *output* (composti da dati scelti e comunicati dalla rete) partecipa all'educazione del figlio impattando, inevitabilmente, sulla sua identità [15]; d'altro canto, l'esperienza digitale del minore può facilmente avvenire al di fuori delle concrete possibilità di controllo dei genitori. Il *libero* accesso al *cyberspazio*, in pratica, produce inevitabilmente un effetto eversivo del principio dell'esclusività educativa dei genitori e istituisce un altro centro di esclusività educativa in capo ai titolari delle piattaforme del *web*, questa volta "oscurato", disincarnato e avvinto dall'analfabetismo emotivo[16].

In definitiva, l'accesso *libero* alla rete del "piccolo minore" sia come attore sia come spettatore [17] confligge con il diritto fondamentale del figlio alla formazione *libera* e *naturale* della sua identità personale. Formazione, che, per essere tale nel concorso di educazione, istruzione e assistenza morale, come ben chiarisce l'art. 315-*bis* c.c., deve essere *rispettosa* della sua personalità.

---

[12] Nel preambolo della Convenzione di New York sui diritti del fanciullo del 20 novembre 1989 si esprime la convinzione «che la famiglia, unità fondamentale della società e ambiente naturale per la crescita e il benessere di tutti i suoi membri e in particolare dei fanciulli, deve ricevere la protezione e l'assistenza di cui necessita per poter svolgere integralmente il suo ruolo nella collettività, riconoscendo che il fanciullo, ai fini dello sviluppo armonioso e completo della sua personalità deve crescere in un ambiente familiare in un clima di felicità, di amore e di comprensione».

[13] Cfr. E. Andreola, *Misure cautelari a tutela dei minori nei* social network, in *Fam. dir.*, 2021, p. 850, la quale osserva che la tutela del minore in questo ambiente «attiene alla garanzia delle prerogative costituzionali della persona (diritto all'immagine, alla riservatezza, all'integrità morale)». V. pure V. Andreoli, *La famiglia digitale. Come la tecnologia ci sta cambiando*, cit., p. 73 ss.

[14] A. Mantelero, *Children online and the future EU data protection framework. Empirical evidences and legal analysis*, in *International Journal of Technology Policy & Law*, 2016, p. 1 ss.

[15] Si veda, in proposito, F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, p. 384 ss.; A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, p. 424.

[16] Su internet come spazio delle emozioni e non dei sentimenti v. U. Galimberti, *L'ospite inquietante. Il nichilismo e i giovani*, Milano, 2007; D. Goleman, *Intelligenza emotiva. Che cos'è e perché può renderci felici*, Milano, 2011.

[17] A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., p. 111; l'a. segnala che «i *social* sono il regno dell'individuale, costruiti secondo la logica dello *spettatore* e questo comporta l'esigenza della spettacolarizzazione di tutto quanto viene comunicato».

2. Internet Free Speech e ruolo educativo dei genitori: il Parental Control System.

È evidente che le tecniche e le tecnologie della rete sono strutturalmente incapaci e, quindi, oggettivamente inidonee ad assolvere la funzione educativa così intesa[18].

Si tratta di un fattore di indubbia rilevanza giuridica atteso che l'interesse del minore ad essere formato in consonanza con il (nel pieno rispetto del) suo concreto *best interest* è oggetto di un diritto fondamentale del figlio, come chiaramente sancito anche dal nostro codice civile all'art. 315 *bis*[19].

È dato comprendere allora che, nell'esperienza digitale del minore (specialmente se "piccolo") governata da una «"sovraesposizione antropologica" della realtà»[20], l'interesse meritevole di protezione consiste nell'apprestare le garanzie, ragionevoli e proporzionate, all'*esclusività dell'educazione*, della responsabilità dei genitori «di allevare il fanciullo e di provvedere al suo sviluppo» (art. 18, par. 1, CNY), anche in termini di possibilità di sorvegliare l'attività *online* del figlio.

Questo dovere di sorveglianza — o meglio, stando agli attuali assetti assiologici del rapporto di filiazione, di vigilanza [21] — costituisce uno dei contenuti irrinunciabili della responsabilità genitoriale[22].

Ma come garantire la vigilanza dei genitori e quindi far salva l'esclusività del loro ruolo educativo, costituzionalmente garantita, e nel contempo tutelare il principio dell'*Internet free speech* esplicitato, con particolare riguardo al minore, dal sistema dei suoi diritti fondamentali? La risposta, oltretutto, va ricercata nella piena osservanza del principio di ingerenza minima dello Stato negli affari familiari, sancito dal sistema degli artt. 29-30-31 Cost.[23].

Ora, se si tratta di tutelare il minore *nella* rete e non *dalla* rete, il primo intervento normativo senz'altro necessario dovrebbe essere volto a non consentire al minore il libero accesso ai contenuti digitali "pericolosi" per lo sviluppo della sua personalità, a quegli spazi, cioè, i cui contenuti confliggono con i valori fondamentali della pacifica convivenza sociale (*fake news*, *hate speech*, *challenges* che incitano all'autolesionismo, pornografia, ecc.[24]).

---

[18] Cfr. G. Garofalo, *Identità digitale e diritto all'oblio: questioni aperte dopo l'approvazione del GDPR*, in *Dir. fam. pers.*, 2021, p. 1506 ss.

[19] Si veda E. Al Mureden e M. Sesta, Sub *art. 315*-bis, in M. Sesta (a cura di), *Codice della famiglia*, III ed., Milano, 2015, p. 1166.

[20] Espressione utilizzata da A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., p. 39 con lo scopo di segnalare «come l'esperienza individuale, con l'avvento delle nuove tecnologie, sia continuamente *sovraesposta* dall'intervento di altri "punti di vista" antropologici, che restano sullo sfondo, mentre ci presentano frammenti di mondo».

[21] R. Senigaglia, *Responsabilità genitoriale e responsabilità dei genitori nella complessità generata (anche) dalla vita sociale digitale*, in *Dir. succ. fam.*, 2022, p. 1031 ss. V. inoltre M. Sesta, *Genitori e figli tra potestà e responsabilità*, in *Riv. dir. priv.*, 2000, p. 238 ss.

[22] In proposito, E. Andreola, *Minori e incapaci in* Internet, Napoli, 2019, p. 107; R. Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità*, cit., p. 80 ss.

[23] P. Zatti, *Rapporto educativo ed intervento del giudice*, in A. Belvedere e M. De Cristofaro (a cura di), *L'autonomia dei minori tra famiglia e società*, Milano, 1980, p. 225; N. Biligotti, *La tutela dei minori nel cyberspazio.* Parental Control *di Stato e libera circolazione dei contenuti: un delicato equilibrio*, in *MediaLaws*, 1/2023, p. 360.

[24] Si veda, in proposito, O. Pollicino, *Fake news, Internet and Metaphors. (To be handled carefully)*, in *MediaLaws*, 2017, p. 23 ss.

Di questi interessi di protezione e della definizione delle loro coordinate tende a farsi carico, nel nostro ordinamento, il d.l. 30 aprile 2020, n. 28 (convertito, con modificazioni, dalla l. 25 giugno 2020, n. 70), il quale impone ai fornitori di servizi di comunicazione elettronica la prestazione di servizi preattivati di sistemi di controllo parentale (d'ora in poi SCP). Segnatamente l'art. 7 *bis*, rubricato "Sistemi di protezione dei minori dai rischi del *cyberspazio*", sancisce che «i contratti di fornitura nei servizi di comunicazione elettronica, disciplinati dal Codice di cui al d.lgs. 1 agosto 2003, n. 259 (n.d.a. Codice delle comunicazioni elettroniche), devono prevedere tra i servizi preattivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore ai diciotto anni».

Tutto ciò in linea con quanto ora sancisce il Reg. (UE) 2022/2065, il quale vincola i fornitori di piattaforme *online* o di motori di ricerca di dimensioni molto grandi ad adottare misure di protezione dei diritti dei minori, tra cui gli strumenti di controllo parentale (art. 35)[25].

Con specifico riferimento ai contenuti ad accesso non libero, in mancanza di apposite previsioni di fonte eurounionale, la selezione compete agli Stati membri[26]. E il referente normativo per l'attuazione dell'art. 7 *bis* d.l. n. 28/2020 è l'art. 37 d. lgs. 208/2021[27], contenente «Disposizioni a tutela dei minori nella programmazione audiovisiva», il quale demanda all'Autorità per le Garanzie nelle Comunicazioni (AGCOM) il compito di fissare i criteri di selezione dei contenuti da ritenere nocivi allo sviluppo della personalità dei minori[28].

Soltanto il 21 gennaio 2023, l'Autorità Garante ha emanato delle linee guida che obbligano gli *internet Service Provider* (ISP) a mettere a disposizione del consumatore, a titolo gratuito e senza alcun costo aggiuntivo, dei sistemi di *parental control*, includendoli e attivandoli nelle offerte dedicate ai minori.

---

[25] Con specifico riferimento agli strumenti di verifica dell'età, la Comunicazione della Commissione su *Un decennio digitale per i bambini e giovani: la nuova strategia europea per un internet migliore per i ragazzi (BIK+)*, COM(2022) 212 final, segnala che «a dispetto di quanto stabilito dal diritto vigente dell'UE (direttiva AVMS e GDPR), i meccanismi di verifica dell'età e gli strumenti che consentono ai genitori di esprimere il loro consenso sono ancora in molti casi inefficaci e agli utenti è spesso richiesto soltanto di inserire la data di nascita al momento della registrazione»; la Commissione si impegna poi a promuovere «strumenti di verifica dell'età sicuri e rispettosi della vita privata, che siano riconosciuti in tutta l'UE» e a collaborare con gli Stati membri, i portatori di interessi pertinenti e gli enti di normazione europei «per rafforzare gli strumenti di verifica dell'età efficaci in via prioritaria».

[26] È chiaro, in questo senso, il considerando 270 della Dir. (UE) 2018/1972, che istituisce il "Codice europeo delle comunicazioni elettroniche", ove precisa che «in mancanza di norme applicabili di diritto dell'Unione, i contenuti, le applicazioni e i servizi sono considerati legali o dannosi ai sensi del diritto nazionale sostanziale e procedurale. Spetta agli Stati membri, e non ai fornitori di reti o servizi di comunicazione elettronica, decidere, seguendo le normali procedure, se i contenuti, le applicazioni e i servizi siano legali o dannosi».

[27] Si tratta del decreto attuativo della Dir. (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato. Con particolare riferimento alle misure di protezione dei minori di età v. F. Donati, *La tutela dei minori nella direttiva 2018/1808*, in *MediaLaws*, 2019, 1, p. 60 ss.

[28] L'ultimo comma dell'art. 7 *bis*, d.l. n. 28/2020 sancisce che «in caso di violazione di obblighi di cui al presente articolo, l'Autorità per le garanzie nelle comunicazioni ordina all'operatore la cessazione della condotta e la restituzione delle eventuali somme ingiustificatamente addebitate agli utenti, indicando in ogni caso un termine non inferiore a sessanta giorni entro cui adempiere».

Le funzioni di attivazione, disattivazione e configurazione del SCP spettano *sempre* all'esercente la responsabilità genitoriale attraverso delle chiavi di accesso fornite direttamente dall'operatore[29].

3. Necessità di differenziare le forme di controllo parentale nell'ambito della minore età.

Le misure di blocco e di filtro dei contenuti attraverso il SCP, così come pensate dal d.l. n. 28/2020 e dalle linee guida dell'AGCOM, sono da ritenersi senz'altro una valida forma di protezione del *best interest* quando si tratta di un "piccolo minore", sprovvisto della capacità di discernimento. Con esse si è inteso articolare una soluzione bilanciata tra *i)* l'interesse dei genitori all'esclusività del ruolo educativo/formativo dell'identità personale del figlio, potendo decidere, nella loro responsabilità, anche di disattivare il sistema di controllo o di attuare una configurazione personale modificando quelle predefinite; *ii)* l'interesse del minore alla costituzione *libera* e *naturale* della sua identità biografica; *iii)* l'interesse del minore all'accesso alla rete, alla sua libertà di espressione, allo sviluppo della propria personalità[30].

Epperò, in termini di proporzionalità e ragionevolezza[31], l'imposizione di servizi preattivati di controllo parentale in *tutti* i casi in cui l'utente sia un minorenne suscita non poche perplessità con riferimento al caso in cui si tratti di un "grande minore", munito della capacità di discernimento e la cui dinamica identitaria ha pressoché abbandonato la funzione *costruttiva* per assestarsi in quella *conservativa*.

Detto altrimenti, non differenziare la minore età nel sacrificare la libertà di espressione e informazione, accusa non poche distonie sistematiche[32].

In pratica, mentre con riferimento al "piccolo minore" sprovvisto della capacità di discernimento la lettura del suo migliore interesse è operata anzitutto dai genitori nel rispetto delle sue capacità, inclinazioni naturali e aspirazioni; relativamente al "grande minore" con capacità di discernimento — che il nostro ordinamento presume al compimento del dodicesimo anno di età

[29] Gli ISP hanno l'obbligo di fornire tutte le informazioni e l'assistenza gratuita per consentire l'attivazione di queste funzioni che comunque deve essere agevole e intuitiva. Deve essere garantita inoltre ampia pubblicità all'obbligo di prestazione di servizi di controllo parentale, non soltanto da parte degli ISP, ma anche degli operatori di telefonia, di reti televisive e di comunicazioni elettroniche.

[30] N. Biligotti, *La tutela dei minori nel cyberspazio.* Parental Control *di Stato e libera circolazione dei contenuti: un delicato equilibrio*, cit., pp. 367-368.

[31] Su questi parametri si rinvia a G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, *passim*. N. Biligotti, *op. cit.*, p. 361, segnala che «se è indubbio, sul piano generale, che la salute psico-fisica dei soggetti minorenni sia un diritto fondamentale titolato ad operare in bilanciamento con altri valori fondamentali (quale, nel caso di specie, la libertà di espressione), è tuttavia necessario prestare particolare attenzione al versante della proporzionalità per quanto attiene alla massima estensione della compressione della libertà fondamentale ritenuta tollerabile, al fine, dall'ordinamento giuridico. Oltrepassato tale stringente confine, ciò che si prospetta è, invero, il conflitto della norma con i principi fondanti dell'ordinamento e, dunque, la sua invalidità costituzionale».

[32] In questi termini L. Lenti, *L'identità del minorenne*, in *L'identità nell'orizzonte del diritto privato*, in *Nuova giur. civ. comm.*, Supplemento al fascicolo 4/2007, p. 66.

(art. 315 *bis* c.c.) — i genitori, dovendo ascoltarlo, sono chiamati a recepire la lettura, *libera* e *informata* che egli conduce del proprio migliore interesse[33].

È nella cornice assiologica del sistema ordinamentale minorile contemporaneo che si inscrive la ragione del dubbio sulla ragionevolezza di una misura rigida di controllo parentale estesa, in termini indifferenziati, alla minore età.

Un diverso metodo accompagna, invece, il *Children's Code* (*Age appropriate design: a code of practice for online services*) dell'Autorità garante inglese per la protezione dei dati personali (ICO, *Information Commissioner's Office*), del 2 settembre 2020.

Con specifico riguardo allo *standard* del *parental control*, il Codice inglese esprime una duplice consapevolezza: da un lato, il forte impatto che la misura di controllo esercita sul diritto del bambino alla vita privata, all'associazione, al gioco, all'accesso all'informazione e alla libertà di espressione; dall'altro, che i minori «*have different needs at different ages*», tanto che a mano a mano che matura la percezione della propria *privacy*, un monitoraggio ostinato dell'attività può essere vissuto dal minore (evidentemente grande) come una restrizione opprimente dello spazio della propria vita privata con inevitabili conseguenze sullo sviluppo e sulla comprensione della propria identità.

Il *Children's Code*, dunque, valorizza la *persona* del minore, differenziando gli obblighi di informazione in ragione dell'età[34] e prevedendo la predisposizione di un segnale evidente (ad es. un'icona luminosa) idoneo a rendere il minore edotto del fatto che la sua attività *online* è monitorata dal genitore.

Una soluzione rigida, che disponga il sistema di controllo parentale nella stessa "misura" per tutta la durata della minore età, solleva, dunque, non pochi dubbi in termini di proporzionalità e ragionevolezza; pare, infatti, imposta dal sistema ordinamentale la necessità di operare una differenziazione in ragione della diversa considerazione della condizione giuridica del minore a seconda che sia sprovvisto o meno della capacità di discernimento.

In sostanza, se nell'età in cui manca il discernimento si giustifica la massima estensione della vigilanza parentale, nell'età del discernimento il suo perimetro va diversamente definito in base alla maturità del figlio che può a sua volta differenziarsi in ragione del contesto, potendo, ad esempio, rivelarsi idonea all'autodeterminazione negli spazi della rete preposti unicamente ad attingere informazioni e non nei *social* network, rispetto ai quali la libertà di quel minore dimostra di accusare il peso del giudizio altrui o di un pensiero polarizzato[35].

---

[33] A.M. McDonald, L. Cranor, *The cost of reading privacy policies*, in *Journal of Law and Policy for the Information Society*, 2008, p. 543 ss.; D.J. Solove, *Introduction: privacy self-management and the consent dilemma*, in *Harvard Law Review*, 2013, p. 1880 ss.; A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo,* cit., p. 410; Id., *L'inconsistente tutela dei minori nel mondo digitale*, cit., p. 528 ss.

[34] Ebbene, proprio al fine di rendere effettive le esigenze di trasparenza e consapevolezza, il *Children's Code* articola delle linee guida sulle informazioni da comunicare e sulle modalità di comunicazione differenziando la disciplina in ragione di cinque fasce in cui suddivide la "stagione" della minore età. Esso individua le seguenti fasce di età al fine di consentire agli operatori dei servizi digitali di valutare ciò che è appropriato per i bambini e le misure di protezione da adottare: 0-5 anni: pre-alfabetizzazione e prima alfabetizzazione; 6-9 anni: età della scuola primaria di base; 10-12 anni: età della transizione; 13-15 anni: prima adolescenza; 16-17 anni: avvicinamento all'età adulta.

[35] Si rinvia, in proposito, a C. Perlingieri, *Social Networks and Private Law*, Napoli, 2017, *passim.*

In definitiva, le ragioni dell'identità personale del minore nel *web*, in cui l'altrove disincarnato sa soltanto profilare e sfruttare ma non "curare" i profili identitari, esigono, senz'altro, l'attivazione di efficaci misure di protezione, conformi, però, alla condizione giuridica del minore, la quale non può prescindere dal suo contesto singolare[36].

[36] Su questi profili teorici, si rinvia a G. ZACCARIA, *Postdiritto. Nuove fonti, nuove categorie*, Bologna, 2022, p. 263 ss.

Tosi E, 'Dati personali e contratto: un ossimoro apparente' (2023) 2 EJPLT, 71 - 92.
DOI: https://doi.org/10.57230/EJPLT232ET

EJPLT
ISSN 2704-8012



Dati personali e contratto: un ossimoro apparente*

Personal data and contract: an apparent oxymoron

EMILIO TOSI
Professore Associato di Diritto Privato
Università di Milano Bicocca
Direttore Esecutivo Centro Studi "Diritto Nuove Tecnologie"

Abstract
L'articolo si concentra sul dibattuto e controverso tema del valore economico e della contrattualizzazione dei dati personali nel quadro giuridico della tutela dei diritti fondamentali della persona e della libertà di circolazione dei dati. I profili di valorizzazione dei dati personali emergono anche nel nuovo Decreto Legislativo 173/2021, che aggiorna il Codice del Consumo in esecuzione della Direttiva UE 2019/770. Inoltre, l'articolo evidenzia la doppia natura personale-economica dei dati riferiti alla persona fisica, e di conseguenza, il consenso al trattamento dei dati nella sua doppia natura, autorizzativa-contrattuale.

The paper focuses on debated and controversial issue of economic value and contractualization of personal data in the legal frame of person fundamental rights protection and freedom of data circulation rights. Personal data exploitation profiles emerge also in new Legislative Decree 173/2021 updating Italian Consumer Code in execution of UE Directive 2019/770. The article also highlights the double nature personal-economic of data referred to the physical person and consequently consent of data processing in its double nature, authorisation-contractual.

*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) 2023, 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: Riservatezza; Data protection; GDPR; Contratto; Dati personali.

Summary: 1. Riservatezza e protezione dei dati personali alla luce del GDPR. – 2. La doppia natura personale e patrimoniale del diritto alla riservatezza e protezione dei dati personali. – 3. Asimmetrie di potere contrattuale e riflessioni sulla fragilità del consenso dell'interessato al trattamento dei dati personali nella società della sorveglianza digitale. – 4. Circolazione dei dati personali tra consenso autorizzatorio e consenso contrattuale. – 5. Patrimonializzazione e monetizzazione dei dati personali alla luce del nuovo art. 135 octies Codice del Consumo. – 6. Dati personali e contratto: una convergenza rimediale opportuna. – 7. L'emersione del contratto di utilizzo dei dati personali e limiti all'autonomia delle parti: un nuovo contratto atipico conformato e regolato.

1. Riservatezza e protezione dei dati personali alla luce del GDPR.

Corre l'obbligo di richiamare il puntuale richiamo dell'illustre Maestro, a cui il presente studio è dedicato: il diritto fondamentale alla riservatezza personale e alla protezione dei dati, spesso per brevità sovrapposti talora persino, erroneamente, confusi, sono invero distinti diritti, seppur strettamente correlati[1].

Si rileva, dunque, una triplice dimensione giuridica della *privacy in senso lato* che può essere compiutamente declinata secondo i seguenti autonomi, ma strettamente correlati, diritti fondamentali: *riservatezza personale, protezione dei dati personali e identità personale*[2].

Nel diritto europeo in materia di protezione dei dati personali emerge una tensione intrinseca, un reciproco bilanciamento, tra diritti fondamentali della persona e libertà della circolazione dei dati personali.

Referente centrale — e prevalente rispetto all'ordinamento interno — è ora, infatti, il *General Data Protection Regulation c.d.* GDPR che disciplina la protezione dei dati personali ma richiamando anche gli altri diritti e libertà fondamentali compresa la libera circolazione dei dati personali.

Tutela dei dati personali e libera circolazione dei dati devono trovare, dunque, necessaria composizione, fermo restando il limite inviolabile del

[1] Così C.M. Bianca, *Diritto civile*, I, *La norma giuridica. I soggetti*, Milano, 2002, p. 180 ss. come nel linguaggio corrente *privacy*, riservatezza personale e protezione dei dati personali siano utilizzati in via alternativa con una certa imprecisione pur essendo diritti distinti protetti dal previgente art. 2 del Codice Privacy ora dal GDPR oltre che dall'art. 2 della Cost. *Cui adde* ID., *Note introduttive,* in *Tutela della privacy. Commentario alla L. 31 dicembre 1996, n. 675*, a cura di Bianca e Busnelli, in *Nuove leggi civ. commentate*, 1999, p. XIX ss.

[2] Sull'autonomìa del diritto alla protezione dei dati personali, diritto alla riservatezza e diritto all'identità personale si vedano: G. Alpa, *Privacy*, in *I precedenti, La formazione giurisprudenziale del diritto civile*, a cura di Alpa, I, Torino, 2000, p. 259 ss.; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e Impresa*, 2017, p. 723 ss.; C.M Bianca, *Diritto Civile*, I, *La norma giuridica. I Soggetti*, Milano, 2002, p. 175 ss.; F.D. Busnelli, *Spunti per un inquadramento sistematico*, in *Tutela della privacy. Commentario alla L. 31 dicembre 1996, n. 675*, a cura di Bianca e Busnelli, in *Nuove leggi civ. commentate*, 1999, p. 228 ss.; *Privacy digitale*, a cura di Tosi, Milano, 2019, *passim;* e da ultimo E. Tosi, *Circolazione contrattuale dei dati personali tra contratto e responsabilità,* Milano, 2023, pp. 78 ss.

rispetto della dignità personale, tutelata dall'art. 2 della Costituzione e dall'art. 1 della Carta di Diritti fondamentali dell'Unione Europea.

Il GDPR all'art. 1 è piuttosto esplicito sul punto statuendo che:

"*1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.*

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

Risulta evidente il principale duplice obbiettivo regolatorio del GDPR che riguarda, da un lato, la protezione dei dati personali delle persone fisiche, indirettamente anche la tutela della riservatezza personale, e dall'altro la loro libera circolazione a livello europeo, in ossequio al già accennato principio di bilanciamento in relazione agli altri diritti fondamentali della persona.

All'ordinamento giuridico spetta, in prospettiva assiologica, in conformità al principio di proporzionalità e meritevolezza, assicurare il giusto bilanciamento tra interessi, contrapposti, del titolare del trattamento e dell'interessato, alla luce dei valori costituzionali interni ed europei[3].

Esplicito nel senso del prospettato bilanciamento tra interessi contrapposti, risulta il considerando n. 4 del GDPR che, in riferimento al difficile equilibrio tra i diritti fondamentali coinvolti nell'àmbito di applicazione delle norme a difesa della privacy, stabilisce il principio secondo cui la relazione tra tutela dei dati personali e altri diritti equiordinati non vada risolta, sempre e comunque, nel senso della prevalenza del diritto alla protezione dei dati personali.

Il considerando 4 del GDPR precisa che "*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*".

---

[3] Con riguardo al principio di proporzionalità si veda P. Perlingieri, *Il diritto civile nella legalità costituzionale*, cit., p. 379 ss., secondo cui tale principio ha valenza quantitativa, è entrato a far parte del nostro ordinamento soprattutto ad opera dell'elaborazione da parte della Corte di Giustizia e trova applicazione ben oltre le materie disciplinate dal diritto europeo, tra elementi di raffronto omogenei. "Viceversa" — osserva l'illustre Autore — "quando il collegamento è tra elementi disomogenei, non comparabili, che coinvolgono interessi non quantificabili, ad esempio, non patrimoniali, ne consegue un bilanciamento tra questi che esige necessariamente una valutazione qualitativa. In tali ipotesi entrano in funzione sia il principio della ragionevolezza sia il principio dell'adeguatezza». I principi di ragionevolezza e adeguatezza sono spesso utilizzati in combinazione con il principio di proporzionalità. Sulla funzione selettiva e di indirizzo del principio di ragionevolezza nelle operazioni di bilanciamento degli interessi, si veda P. Femia, *Interessi e conflitti culturali nell'autonomia privata e nella responsabilità civile*, Napoli, 1996, p. 158 ss. e p. 516 ss. Sul tema del bilanciamento secondo ragionevolezza si veda per tutti: G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, p. 102 ss.; da ultimo F. Bravo, *Il «diritto» a trattare dati personali nello svolgimento dell'attività economica, Padova, 2018.*

Non trattandosi di prerogativa assoluta dell'individuo allora il rispetto di tali diritti fondamentali — riservatezza, protezione dei dati e identità personale — deve essere necessariamente bilanciato con interessi di pari grado confliggenti, in applicazione del principio di proporzionalità e meritevolezza.

Pare in ogni caso doversi condividere "*la prevalenza del riconoscimento e della garanzia dei diritti inviolabili della persona umana su altri istituti pur definiti fondamentali, ma non inviolabili (ad esempio, il diritto di proprietà intellettuale)"*[4].

La giurisprudenza eurounitaria è, invero, piuttosto, incline a dare prevalenza al diritto alla protezione dei dati personali rispetto agli altri diritti equiordinati ovvero consistenti in un diritto della personalità o in un altro diritto o libertà fondamentale, affermando il carattere eccezionale delle limitazioni ad esso poste[5].

Non mancano, tuttavia, pronunce di segno contrarie più attente al bilanciamento rispetto a diritti equiordinati[6].

Ma alla luce del citato considerando n. 4 del GDPR non si può sottacere l'apertura di una nuova linea di interpretazione in riferimento al difficile equilibrio tra i diritti fondamentali coinvolti nell'àmbito di applicazione delle norme in difesa della privacy.

La relazione tra tutela dei dati personali e altri diritti fondamentali non deve risolversi necessariamente nel senso della prevalenza del diritto alla protezione dei dati personali, non trattandosi di prerogativa assoluta: semmai pare corretto e ragionevole ritenere che il rispetto di tale diritto vada messo in relazione con la sua funzione sociale e con la necessità di contemperarlo con gli eventuali diritti di pari grado confliggenti, in ottemperanza al principio di proporzionalità, primo fra tutti il principio di libera intrapresa e circolazione dei dati[7].

---

[4] Cosi P. Perlingieri, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro Napoletano*, 2018, p. 481 ss. che, inoltre, valuta positivamente il fatto che il GDPR contenga il richiamo a principi di valenza generale caratterizzanti l'intero sistema ordina mentale, quali il principio di proporzionalità, di cui, appunto, al considerando n. 4 del regolamento e il principio di sussidiarietà, espressamente confermato dal considerando n. 170 del regolamento, il quale dispone che: "Poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE)".

[5] Corte Giustizia UE, 13 maggio 2014, C-131/2012, Google Spain 3L c. Agencia Espniola de Proteccion de Datos, in *Foro it.*, 2014, IV, c. 295, con nota di A. Palmieri-R. Pardolesi, *Diritto all'oblio: il futuro dietro le spalle;* Corte Giustizia UE, 6 ottobre 2015, C-362/14, Schrems c. Data Protection Commissioner.

[6] *Contra* Corte Giust. UE, 29 gennaio 2008, C-275/06, *Promusicae* in *Giur. it.*, IV, 2009, c. 509 ss., con nota di M.L. Gambini, *Diritto d'autore e tutela dei dati personali: una difficile convivenza in Rete*; Corte Giust.; UE, 24 novembre 2011 (C-468/2010 e C-469/2010, ASNEF e FECEMD c. Administracidn del Estrada; e, da ultimo, Corte Giustizia marzo 2017, C-398/15, CCIAA Lecce, in *Foro it.*, 2017, 4, c. 177 ss., con nota di R. Pardolesi, *Non c'è diritto all'oblio per i dati personali nel registro delle imprese. O forse si'*, che ritiene prevalente l'interesse alla pubblicità delle informazioni contenute nei registri delle imprese rispetto all'interesse individuale all'oblio di informazioni personali pregiudizievoli e non più attuali.

[7] Emerge, quindi, la dimensione relazionale del modello europeo della tutela della privacy come sottolineato in dottrina da: R. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 583 ss.; ID., *Tecnologie e diritti*, Bologna, 1995, 49, secondo cui: "Non si tratta solo di scegliere tra valori contrapposti, facendo prevalere seccamente l'uno l'altro. Bisogna procedere a più complessi bilanciamenti tra gli interessi in gioco, per assicurare insieme la garanzia dei diritti individuali e la progressiva apertura della società»; F.D. Busnelli, *Spunti per un inquadramento sistematico*, *Tutela della privacy. Commentario alla L. 31 dicembre 1996, n. 675*, a cura di Bianca e Busnelli, in *Nuove leggi*

2. La doppia natura personale e patrimoniale del diritto alla riservatezza e protezione dei dati personali.

Ai fini della presente indagine — secondo una condivisibile distinzione dottrinale — intendiamo considerare esclusivamente i *diritti della personalità morale* — in particolare, i diritti sugli attributi *immateriali della persona* suscettibili di oggettivazione quale il nome, l'immagine, l'identità personale, identità digitale e in particolare i *dati personali* — non anche i *diritti della personalità fisica*[8].

Il diritto alla protezione dei dati personali, alla riservatezza e all'identità personale rientrano, quindi, tra le situazioni giuridiche soggettive qualificabili come diritti della personalità — autonomi in ossequio alla preferibile teoria pluralistica — finalizzate alla valorizzazione della dignità e dell'autodeterminazione della persona umana espressione di facoltà e poteri su qualità materiali e immateriali che concorrono a delineare l'individualità della persona, la personalità appunto, i cui tratti distintivi sono classicamente individuati nella indisponibilità, intrasmissibilità, irrinunciabilità, imprescrittibilità ed insurrogabilità[9].

Diritti fondamentali della personalità che assumono anche rilevanza *meta-individuale* in quanto precondizione per la piena fruizione dei diritti di libertà individuale — e collettiva — della persona umana correlata all'esercizio dei diritti civili, sociali e politici, in ultima istanza per il buon funzionamento dell'ordinamento democratico[10].

Ai predetti tratti qualificanti non è scontato, almeno limitamente ai diritti sugli attributi *immateriali* della personalità, che si debba aggiungere, come potrebbe ritenersi in base, a una lettura dottrinale rigorosa e tradizionale, anche l'elemento qualificante della non commerciabilità e non patrimonialità: la questione è, invero, controversa[11].

---

civ. commentate, 1999, p. 228 ss.; G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. inf.*, 1997, p. 703 ss.

[8] Così G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, 4 ss.; cui *adde amplius* G. ALPA- G. RESTA, *Le persone fisiche e i diritti della personalità, I*, in *Trattato di Diritto Civile*, diretto da Sacco, Torino, 2006, *passim*, spec. P. 87 ss.

[9] Si veda per tutti C.M. BIANCA, *Diritto civile*, I, *La norma giuridica. I soggetti*, Milano, 2002, 139 ss., spec. P. 147 ss.

[10] Così S. RODOTÀ, *La* privacy *tra individuo e collettività*, in *Tecnologie e diritti*, Bologna, 1995, p. 24 ss. che riconosce al *Codice privacy* la natura di vero e proprio statuto generale della persona; *cui adde* da ultimo S. RODOTA', *Intervista su* privacy *e libertà*, a cura di Conti, Bari, 2005. Nello stesso senso anche M.L. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli, 2018, p. 20 ss.

[11] Si veda *amplius G.* ALPA-ANSALDO, *Le persone fisiche, artt. 1-10*, in Codice Civile. Commentario diretto da P. Schelsinger, Milano, 1996; P. PERLINGIERI, *La persona e i suoi diritti, Problemi di diritto civile*, Napoli. 2005, p. 3 ss.; P. RESCIGNO, *Personalità (Diritto della)*, in *Enc. Giur. Treccani*, XXII, Roma, 1991, p. 5 ss.; D. MESSINETTI, *Personalità (diritti della)*, in *Enc. dir.*, XXXIII, Milano, 1983, p. 355 ss.; A. DE CUPIS, *I diritti della personalità*, in *Trattato Diritto Civile e Commerciale*, diretto da Cicu-Messineo, continuato da Mengoni, 2° ed., Milano, 1982; V. ZENO ZENCOVICH, *Personalità (Diritti della*), in Digesto disc. Privatistiche, sez. civile, *XIII, Torino, 1996, p.* 431 ss*;* RESTA, *Diritti della personalità: problemi e prospettive*, in *Riv. Dir. Inf. e informat.*, 2007, 1043 ss.; FERRI, *Persona e formalismo giuridico*, Rimini, 1985; P.VERCELLONE, *voce* Personalità (diritti della), *Novissimo Digesto Italiano*, XII, Torino, 1965; e da ultimo V. ZENO ZENCOVICH, *I diritti della personalità*, in *Trattato di Diritto Civile*, diretto da N. Lipari e P. Rescigno, coordinato da A. Zoppini, I, Fonti — Soggetti — Famiglia, tomo I, Le Fonti e i Soggetti, Milano, 2009, 496 ss.; ID., *Profili negoziali degli attributi della personalità, Dir. Informaz. e informatica*, 1993, p. 545 ss.

In un contesto di incertezza teorica e normativa, pare, invero, preferibile, come suggerito efficacemente da attenta dottrina, in quanto più adeguato ad inquadrare il fenomeno, il tentativo di comporre il rapporto tra patrimonialità e non patrimonialità secondo il seguente duplice scenario sostanziale[12]:

— gli attributi immateriali della personalità possono essere oggetto di interessi non patrimoniali e patrimoniali. Tuttavia, sono solo gli interessi non patrimoniali a rientrare nell'ambito protettivo della lettura costituzionale del diritto fondamentale della personalità e soggetti ai limiti negoziali correlati;

— il diritto che ciascun soggetto ha sulla propria personalità, o singoli attributi di essa, può avere una duplice connotazione, patrimoniale e non patrimoniale, ciascuna regolata da criteri propri.

La patrimonialità non pare, quindi, elidere il diritto della personalità ma risulta compatibile - nei limiti del prevalente rispetto del principio costituzionale, questo sì non solo assoluto ma anche inviolabile, di dignità della persona - secondo il paradigma analogico delineato dal diritto d'autore in cui risulta netta la distinzione tra diritto morale alla paternità dell'opera e diritto economico di sfruttamento della stessa.

Anche nello schema del *right to privacy* nord-americano si incardinano da un lato l'interesse non patrimoniale alla tutela dell'intangibilità della persona, dall'altro, seppur implicitamente, quello patrimoniale alle aspettative di profitto connesse allo sfruttamento economico dell'identità[13].

Certo i diritti di esclusiva sui beni immateriali sono, di regola, tipizzati dal legislatore: nel caso del diritto d'autore l'oggetto del diritto non è la persona ma un'opera intellettuale della medesima, il frutto della creatività della persona su cui si innervano, sinteticamente, da un lato il diritto morale alla paternità dell'opera e dall'altro, diritti correlati allo sfruttamento economico della stessa.

Similmente ai diritti di esclusiva sui beni immateriali tipizzati dal legislatore, nel caso del diritto alla protezione dei dati personali l'oggetto del diritto disponibile non è certamente la persona né il diritto della personalità ma il diritto di godimento temporaneo del dato personale riferito — direttamente o indirettamente — alla medesima che viene sfruttato economicamente per la profilazione dei consumatori e per eterogenee finalità innovative correlate all'economia dei *big data*[14].

Di tal guisa che gli attributi immateriali della personalità costituirebbero un nuovo bene giuridico immateriale, senza entrare nel merito del dibattito tra logica proprietaria e obbligatoria, che esula dall'economia del presente studio, sul quale il titolare potrebbe vantare diritti di contenuto extrapatrimoniale e anche patrimoniale.

Con riguardo ai primi la tutela sarà quella *erga omnes* dei diritti assoluti; con

---

[12] Così V. Zeno Zencovich, *I diritti della personalità*, in *Trattato di Diritto Civile*, diretto da N. Lipari e P. Rescigno, coordinato da A. Zoppini, I, Fonti — Soggetti — Famiglia, tomo I, *Le Fonti e i Soggetti,* Milano, 2009, p. 516.

[13] G. Resta, *Autonomìa privata e diritti della personalità*, Napoli, 2005, p. 213; *cui adde Diritti esclusivi e nuovi beni immateriali,* a cura di Resta, Torino, 2010; A. Gambaro, *I beni, in Trattato di Diritto Civile e Commerciale*, Milano, 2012, *passim.*

[14] 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,* p. 363 ss.

riguardo ai secondi quella negoziale *inter partes* di natura contrattuale[15].

Anche se pare di poter, a ragion veduta, ritenere largamente preferibile l'opzione interpretativa che rifugge la logica proprietaria prediligendo la natura obbligatoria: occorre considerare, invero, non solo la possibilità che i dati personali, in determinate circostanze possano essere utilizzati a mente dell'art. 6 del GDPR anche senza consenso autorizzatorio dell'interessato, ma anche il modello circolatorio elettivo contrattuale che si fonda proprio sullo sfruttamento economico, non esclusivo e temporaneo, da parte di molteplici operatori commerciali nella società della condivisione.

Va registrato, inoltre, che l'evoluzione della società della sorveglianza e dei mercati digitali progressivamente attenua alcune delle caratteristiche tradizionalmente attribuite ai diritti della personalità: si pensi proprio alla progressiva patrimonializzazione degli attributi immateriali tutelati da questi diritti ed alla conseguente loro, almeno parziale, disponibilità, compatibilmente con la natura di diritti fondamentali della persona e nei limiti dei precetti conformativi delineati dal GDPR[16].

Si segnala, infine, per completezza, anche la posizione originale di altra dottrina che ravvisa — in prospettiva squisitamente individualistica e proprietaria — un nuovo bene immateriale oggetto di un diritto esclusivo, riconducibile alla categoria dei diritti di proprietà intellettuale, da parte del titolare[17].

In tale prospettiva si potrebbe persino ipotizzare, *de iure condendo*, la tipizzazione di un nuovo diritto per lo sfruttamento commerciale dei dati personali: un nuovo diritto economico remunerativo dell'interessato a fronte del conferimento dei dati personali nelle grandi banche dati globali per l'utilizzo ai fini di profilazione consumeristica e di *business analytics* tipiche dell'economia dei *big data*.

Si tratta di una proposta provocatoria, ma non troppo, di valorizzazione *de iure condendo* del patrimonio informativo personale sulla falsariga del modello delineato dalla Legge sul Diritto d'Autore (LDA) per i molteplici diritti connessi in materia di proprietà intellettuale: si pensi — a titolo esemplificativo — in particolare all'art. 102-*bis* LDA che prevede un diritto di sfruttamento economico a favore del costitutore di banca dati.

Corre l'obbligo, infine, di evidenziare che l'interesse generale alla liceità,

---

[15] C. SCOGNAMIGLIO, *Il diritto all'utilizzazione economica del nome e dell'immagine delle persone celebri*, in *Riv. Dir. Infor. e Informatica*, 1988, p. 1 ss. In senso critico V. ZENO ZENCOVICH, *op. ult. cit.*, p. 516 secondo cui tale interpretazione si scontrerebbe con uno dei capisaldi del vigente sistema dei beni in base al quale solo la legge può prevedere le regole di esclusiva sui beni immateriali e dunque i limiti entro i quali si può disporre del diritto a favore di terzi.

[16] Si vedano sul punto secondo diverse linee interpretative inclini ad ammettere patrimonialità e disponibilità, entro limiti più o meno ampi comunque non lesivi della dignità della persona e compatibili con la normativa in materia di trattamento dei dati personali (allora solo il Codice Privacy e ora innanzitutto il GDPR): G. ALPA- G. RESTA, *Le persone fisiche e i diritti della personalità*, I, in *Trattatoo di Diritto Civile*, diretto da R. Sacco, Torino 2006, *passim*, spec. P. 629 ss.; G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005; MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001; V. ZENO ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Dir. inf.*, 1993, 545 ss.; M.L. GAMBINI, *Dati personali e Internet*, Napoli, 2008; C. PERLINGIERI, *Profili civilistici dei social networks*, Napoli, 2014, *passim* ma spec. P. 84 ss.; C. MIGNONE, *Identità della persona e potere di disposizione*, Napoli, 2014; da ultimo: F. BRAVO, *Il "diritto" a trattare dati perosnali nello svolgimento dell'attività economica*, Padova, 2018, *passim;* e RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella riscostruzione del fenomeno*, in *Dir. Informaz. e informatica*, 2018, p. 689 ss.

[17] L.C. UBERTAZZI, *Riservatezza informatica ed industria culturale*, in *AIDA*, 1997, 530 ss.

correttezza e trasparenza del trattamento dei dati personali della collettività si affianca e persino sovrasta il diritto fondamentale, individuale, dell'interessato alla protezione dei propri dati personali e viene tutelato prioritariamente e a prescindere dai pregiudizi che possano derivare ai diritti dei singoli interessati dai trattamenti effettuati[18].

Secondo parte della dottrina il positivo superamento della prospettiva prevalentemente individuale che ha finora caratterizzato la disciplina europea di cui alla Direttiva CE 95/46 e nazionale sulla protezione dei dati personali avrebbe dovuto essere perseguito in termini ancora più penetranti e decisi, affidando la tutela dei diritti individuali della persona rispetto al trattamento dei dati personali in accentuata prospettiva collettiva-pubblicistica[19].

Prospettiva collettiva-pubblicistica che pare essere necessario contrappeso e forza di riequilibrio decisiva delle strutturali asimmetrie di potere informativo, economico e contrattuale – ancora più accentuate dalle potenziali evoluzioni correlate alla diffusione delle Artificial Intelligence (AI) - che caratterizzano i rapporti giuridici intercorrenti tra titolare del trattamento e persona-interessato-consumatore, soggetto debole meritevole di protezione da parte dell'ordinamento giuridico[20].

Accentuate asimmetrie di potere che rendono sempre più fragile il consenso individuale.

Invero, la protezione dei dati personali, come si illustrerà ulteriormente *infra,* non passa più - *rectius* non passa più esclusivamente e principalmente - attraverso la logica squisitamente individuale dell'*autodeterminazione informativa* fondata sul *consenso autorizzatorio informato* da parte della singola persona fisica.

3. Asimmetrie di potere contrattuale e riflessioni sulla fragilità del

[18] Si veda in tal senso: R. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016, 4/1, p. 49 ss.

[19] Così A. MANTELERO, *Responsabilità e rischio nel Regolamento UE n. 2016/679*, in *Nuove leggi civ. commentate*, 2017, p. 152 ss. Si vedano inoltre sul tema: L. GATT, *Rapporto possibile tra atipicità dell'illecito ed esimenti della concezione bianchiana della responsabilità quale tutela civile contro l'illecito: il caso del trattamento abusivo di dati personali,* in *M. Bianca* (a cura di), *La responsabilità. Principi e funzioni. Continuando a dialogare con Cesare Massimo Bianca, Quaderni della Rivista di diritto civile* n. 31, Wolters Kluwer, Milano 2023, pp. 345-351; E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR, Milano, 2019, passim.*

[20] Nel senso di una progressiva convergenza e in ordine all'applicabilità, in prospettiva di tutela collettiva, della normativa consumeristica all'interessato dal trattamento dati personali veda sentenza della Corte di Giustizia UE del 28 aprile 2022 relativa alla causa C319/20 secondo cui: "L'articolo 80, paragrafo 2, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 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), deve essere interpretato nel senso che esso non osta ad una normativa nazionale che consente ad un'associazione di tutela degli interessi dei consumatori di agire in giudizio, in assenza di un mandato che le sia stato conferito a tale scopo e indipendentemente dalla violazione di specifici diritti degli interessati, contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, facendo valere la violazione del divieto di pratiche commerciali sleali, la violazione di una legge in materia di tutela dei consumatori o la violazione del divieto di utilizzazione di condizioni generali di contratto nulle, qualora il trattamento di dati in questione sia idoneo a pregiudicare i diritti riconosciuti da tale regolamento a persone fisiche identificate o identificabili".

consenso dell'interessato al trattamento dei dati personali nella società della sorveglianza digitale.

Le asimmetrie di potere si cristallizzano plasticamente nel rapporto asimmetrico tra big tech titolare del trattamento e persona fisica interessata dal trattamento.

Si registra dunque l'emergente progressiva *fragilità del consenso* della persona fisica interessata dal trattamento di dati personali, nella società digitale, di fronte alla pervasività dei *digital player globali* e dei *big data* che pure risulta esplicitata nell'ordito regolatorio europeo del GDPR.

L'art. 4 del GDPR stabilisce che per consenso dell'interessato al trattamento debba intendersi qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato.

Tuttavia l'efficacia della tutela dei dati personali non passa più principalmente attraverso il *consenso informato* al trattamento da parte dell'interessato che, quindi, perde rilievo, viene depotenziato dalla *società del capitalismo della sorveglianza digitale*[21].

Il consenso al trattamento dei dati personali deve, pertanto, per essere davvero giuridicamente rilevante — *rectius* informato e libero, soprattutto *consapevole* — comprendere anche l'algoritmo stesso che deve, quindi, essere disvelato e rivelato, reso trasparente agli utilizzatori della piattaforma digitale.

Il profilo della libertà del consenso, come si è già osservato, è particolarmente critico in un contesto fortemente asimmetrico come quello dei mercati digitali in cui tale strumento protettivo riuslta inidoneo, per certi aspetti defatigante per l'interessato nella forzata reiterazione necessaria per accedere ai servizi e contenuti digitali, così rischiando di ridursi a mera *fictio*.

D'altra parte è lo stesso GDPR nel considerando 43 a precisare che "*libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento*".

Quindi il mero utilizzo del *consenso autorizzatorio informato* nei *rapporti asimmetrici* da cui risulti *evidente squilibrio* è ritenuto inopportuno, dallo stesso legislatore europeo, proprio perché insufficiente a proteggere l'interessato.

La manifestazione di volontà "libera" implica che l'interessato abbia la possibilità di operare una scelta effettiva ed esercitare il controllo sui propri dati personali.

Il GDPR stabilisce in proposito che, se l'interessato non dispone di una scelta effettiva o si sente obbligato ad acconsentire oppure subirà conseguenze negative se non acconsente, il consenso non potrà ritenersi valido.

Se il *consenso* è un elemento non negoziabile delle condizioni generali di contratto, si presume che non sia stato prestato liberamente. Di conseguenza, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio.

Nel valutare se il consenso al trattamento dei dati sia stato prestato

[21] S. ZUBOFF, *Big other: surveillance capitalism and the prospects of an information civilization, in Journal of Information Technology,* 2015, 30 ss; e da ultimo: ID., *Il capitalismo della sorveglianza*, Roma, 2019. Si veda anche *Garante per la Protezione dei dati personali, La società sorvegliata*, Atti del Convegno 28 gennaio 2016, Roma, 2016.

liberamente, si deve anche tenere nella massima considerazione l'eventualità – tra le altre - che l'esecuzione di un contratto o la prestazione di un servizio sia condizionata alla prestazione del consenso al trattamento di dati personali non necessari all'esecuzione del contratto (art. 7, paragrafo 4, GDPR).

L'inciso "tra le altre" sottindende qualsiasi azione di pressione o influenza inappropriata sull'interessato (che si può manifestare in vari modi) che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido (sentenza CGUE 11 novembre 2020 caso *Orange România SA)*.

Si affiancano, opportunamente, nel quadro regolatorio introdotto dal GDPR ulteriori, più efficaci, parametri di liceità del trattamento quali il *consenso contrattuale*, l'obbligo di legge o più in generale il *legittimo interesse* (art. 6 GDPR).

Nella società digitale la *protezione del dato personale*, dunque, non risiede — o almeno non più solo e principalmente — nel consenso individuale che di per sè non è più in grado di proteggere l'interessato soggetto debole del rapporto asimmetrico del trattamento dei dati personali. La tutela dell'interessato semmai discende da un quadro complesso di regole protettive e conformative inderogabili poste a carico di ogni titolare di trattamento dei dati personali fondato su altri più efficaci strumenti privatistici e pubblicistici anche di natura deterrente e sanzionatoria.

L'asimmetria di potere (informativo, tecnologico, economico e normativo) tra i soggetti del trattamento (titolare-interessato) conferma la bontà di una lettura assiologica, costituzionalmente orientata, della tutela della riservatezza e della protezione dei dati personali — centrata sulla tutela dei diritti fondamentali della persona offerta dall'art. 2 della Costituzione italiana oltre che dagli artt. 1, 7 e 8 della *Carta dei diritti fondamentali* UE — che, attraverso il prisma delle fonti interne ed eurounitarie, consenta di dare piena efficacia a tali fondamentali diritti, offrendo un saldo appiglio per non soccombere di fronte alle plurime e cangianti pressioni mercatorie della società liquida digitale.

Si pensi all'imposizione da parte del GDPR in capo al Titolare di *obblighi di gestione preventiva e differenziata* — sotto il profilo quantitativo e qualitativo — del rischio correlato al trattamento, ai principi di trasparenza, di accountability e sicurezza: questi sono i nuovi, più efficaci, strumenti normativi europei posti a presidio dell'osservanza dei parametri di liceità e correttezza che illuminano tutto il processo del trattamento nel complesso bilanciamento dei diritti fondamentali della persona e dei diritti delle imprese alla libera circolazione dei dati personali.

Infine, la protezione dell'interessato, soggetto debole rispetto al titolare del trattamento, passa pur sempre anche attraverso i principi generali di buona fede in senso oggettivo, proporzionalità, regionevolezza e soprattutto meritevolezza delle finalità di trattamento, particolarmente efficaci anche nel contesto applicativo di cui trattasi[22].

4. Circolazione dei dati personali tra consenso autorizzatorio e consenso contrattuale.

[22] P. Perlingieri, *Privacy digitale e protezione dei dati personali tra persona e mercato*, cit., *passim; cui adde* G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, cit., *passim.*

Si discute relativamente alla libertà negoziale di disporre dei propri dati personali per finalità economiche altre rispetto a quelle connaturate al servizio richiesto dall'interessato.

Se gli interessi che l'autonomia contrattuale intende soddisfare con la creazione di tale nuovo modello contrattuale *atipico* sono meritevoli di tutela ex art. 1322 c.c. nulla pare ostare in ordine alla validità del contratto né sotto il profilo civilistico né ai sensi del GDPR.

Si tratta del problema giuridico sotteso al rilevante fenomeno dei *big data* che richiede ai *digital player* di analizzare in *cluster dati* di utenti e consumatori per le più svariate finalità — di marketing, di sviluppo di nuovi servizi personalizzati e così via — dati in relazione ai quali l'interessato è chiamato ad esprimere un *consenso* al trasferimento dei propri dati e allo sfruttamento economico degli stessi, oltre, quindi, il mero consenso al trattamento previsto dall'art. 6.1 lett. a) del GDPR.

Si tratta, invero, di esprimere il consenso in ordine all'utilizzo dei propri dati personali per lo sfruttamento economico degli stessi da parte dei *digital player*: attività di trattamento sempre, tuttavia, condizionata — anche in presenza del consenso dell'interessato — all'osservanza delle regole conformative e delle procedure delineate dal GDPR da parte del Titolare del trattamento.

Si registra con il dupplice fenomeno della patrimonializzazione e monetizzazione dei dati personali l'emersione della doppia natura del consenso al trattamento dei dati stessi:

— *consenso autorizzatorio* sotto il profilo del trattamento dei dati personali in senso stretto per finalità economiche diverse da quelle relative al servizio richiesto espressione del *potere di autodeterminazione informativa* della persona interessata dal trattamento[23]; ma anche

— *consenso contrattuale* per consentire non solo il trattamento dei dati personali necessari all'esecuzione del contratto di fornitura di beni e servizi ma anche lo sfruttamento economico dei propri dati personali quando l'oggetto del contratto sia proprio il trattamento dei dati personali dell'interessato e non altro[24].

La duplice natura del consenso — personale-non patrimoniale nell'ambito

---

[23] D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Rivista critica di diritto privato*, 1998, spec. p. 353 secondo cui il consenso al trattamento avrebbe carattere di "permesso autorizzativo" con efficacia costitutiva nell'altrui sfera (personale). Più in generale sul negozio autorizzatorio: D. AURICCHIO, voce *Autorizzazione (dir. priv.)*, in *Enciclopedia del diritto*, IV, Milano, 1959, p. 502 ss.; M. TAMPONI, *L'atto non autorizzato nell'amministrazione dei patrimoni altrui*, Milano, Giuffrè, 1992, p. 28 ss.

[24] Sul tema del consenso e sulla controversa natura autorizzatoria o anche negoziale si vedano: G.ALPA-G.RESTA, *Le persone fisiche e i diritti della personalità, I*, in *Trattato di Diritto Civile*, diretto da R. Sacco, Torino 2006, *passim*, spec. p. 629 ss.; F.BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in questa *Rivista*, 2019, p. 34 ss.; ID., *La compravendita di dati personali?, Diritto di Internet*, 2020, II, p. 521 ss.; ID, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, *passim; P.* MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001; e V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. Informaz. e informatica*, 2018, p. 689 ss.; A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, p. 184 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali,* Torino, 2021, *passim*; P. GALLO, *Il consenso al trattamento dei dati personali come prestazione,* in *Riv. Dir. Civ.,* 2022, pp. 1054 ss.; T.M. UBERTAZZI, *Ripensando alla revoca del consenso nella prospettiva funzjonale della privacy, in Contratto e impresa, 2022*, pp. 27 ss.; S. ORLANDO, *Per un sindacato di liceità del consenso,* in *Persona e mercato,* 2022, pp. 527 ss. e da ultimo E. TOSI, *Circolazione contrattuale dei dati personali tra contratto e responsabilità,* op. cit., pp. 78 ss.

delle condizioni di liceità del trattamento ascrivibili esclusivamente al potere di autodeterminazione informativa unilaterale dell'interessato e contrattuale-patrimoniale nell'ambito delle condizioni di liceità del trattamento basata su contratto *rectius* su rapporto giuridico bilaterale — non è peregrina, anzi.

Proprio nel GDPR si ammette che possa non essere richiesto uno specifico e autonomo consenso al trattamento, nell'ipotesi in cui quest'ultimo sia stato già prestato dall'interessato in fase contrattuale — o precontrattuale — ossia quando, in buona sostanza, il trattamento sia necessario per l'esecuzione di un contratto tra Titolare e l'interessato o costituisca oggetto di una richiesta precontrattuale dell'interessato (art. 6, par. 1 lett. *b*) GDPR).

Tuttavvia pur a fronte della doppia natura del consenso non si ravvisa necessità di esprimere un doppio consenso cumulativo uno per il trattamento e uno per il contratto: sono consensi, invero, di regola alternativi tra loro, che si cumulano solo nel limitato caso in cui oltre al trattamento dei dati personali necessari all'esecuzione del contratto si richieda un trattamento degli stessi dati ma per finalità ulteriori, altre rispetto all'esecuzione del contratto.

Il consenso autorizzatorio dell'interessato (art.6 lett. a) del GDPR) e il consenso contrattuale sono, pertanto, basi giuridiche legittime, corre l'obbligo di ribadire per chiarezza, alternative tra loro (art.6 lett. b) del GDPR).

Il consenso contrattuale altrettanto libero di quello autorizzatorio pare, invero, idoneo ad assorbire, per tale, ragione anche il consenso autorizzatorio: ovviamente solo nel caso in cui il predetto consenso contrattuale riguardi dati personali necessari per l'esecuzione del contratto oppure quando il contratto abbia proprio ad oggetto il trattamento dei dati personali dell'interessato e non altri servizi digitali.

In difetto si ritorna alla regola del consenso autorizzatorio espressione del potere di autodeterminazione dell'interessato per le finalità ulteriori rispetto a quelle oggetto del contratto.

L'emersione della patrimonializzazione delle attività di trattamento dati personali richiede, dunque, di non eludere la questione sottraendosi alla facile tentazione di ancorarsi a tradizionali impostazioni dogmatiche meramente ostative al fenomeno globale richiamato e in ultima istanza preclusive - in prospettiva consumeristica oltre i ristretti confini del GDPR - al rafforzamento dei rimedi protettivi per il soggetto interessato dal trattamento.

È tempo, semmai, di superare le resistenze dogmatiche tradizionali in ordine al possibile rilievo anche contrattuale del consenso in materia di dati personali — che parte della dottrina più tradizionalista ancora disconosce — non solo autorizzatorio quindi per prendere atto e governare, *rectius* proteggere efficacemente il soggetto debole del rapporto asimmetrico con opportuno strumento rimediale, di natura contrattuale, ulteriore rispetto a quello settoriale previsto per altre finalità dal GDPR[25].

---

[25] V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, cit., p. 95 ss.; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella riscostruzione del fenomeno*, in *Dir. inform.*, 2018, p. 689 ss.; F. BRAVO, *Il «diritto» a trattare dati personali nello svolgimento dell'attività economica, cit.;* I. A. CAGGIANO, Il consenso *al trattamento dei dati personali nel nuovo Regolamento Europeo. Analisi giuridica e studi comportamentali*, Osservatorio del diritto civile e commerciale, 2018, n. 1, p. 67; S. TOBANI, *Diritti della personalità e contratto. Dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Torino, 2019; G. VERSACI, *La contrattualizzazione dei dai personali dei consumatori*, Napoli, 2020; A.

La progressiva valorizzazione dei dati personali in termini negoziali si declina, in dottrina, ora in termini di diritti della personalità immateriale suscettibili di circolazione contrattuale in quanto rientranti nella sfera personale di pertinenza e disponibilità dell'interessato [26] oppure, da altra prospettiva, evidenziando l'efficacia derivativo-costitutiva dell'atto funzionale allo sfruttamento economico di attributi individuali della personalità immateriale mutuando, per analogia, la struttura negoziale del contratto di licenza nell'ambito del diritto d'autore[27].

E' ormai evidente a tutti la progressiva patrimonializzazione dei dati personali, in linea con lo sdoppiamento peculiare dei diritti della personalità immateriali: i dati personali hanno un valore economico significativo e non di rado sono utilizzati quale "corrispettivo" per fornitura di contenuti digitali o prestazioni di servizi digitali e "cessione" del diritto di sfruttamento economico - *temporaneo e non esclusivo* - dei propri dati personali eteroconformata ai precetti inderogabili del GDPR.

I contenuti digitali e i servizi digitali sono, infatti, spesso forniti online nell'ambito di contratti che non prevedono, da parte del consumatore, il pagamento di un prezzo, bensì la mera comunicazione di dati personali al prestatore di servizi digitali[28].

Si ribadisce, pertanto, che disconoscere tale fenomeno socio-economico rinunciando ad inquadrarlo correttamente dal punto di vista giuridico non produrrebbe altro che un *deficit* rimediale che al contrario deve essere offerto — rafforzato e non indebolito — all'interessato dal trattamento dei dati assecondando la convergenza normativa emergente tra protezione dati personali-protezione consumatori[29].

Le segnalate preclusioni dogmatiche alla circolazione dei dati personali sono, invero, il frutto di un vero e proprio *equivoco interpretativo* conseguenza di una lettura non sistematica del GDPR da cui si evince semmai, corre l'obbligo di sottolineare ancora una volta, proprio il contrario. Si disconosce,

---

C. DI LANDRO, *Big Data. Rischi e tutele nel trattamento dei dati personali*, Napoli, 2020; e da ultimo E. TOSI, *Circolazione contrattuale dei dati personali tra contratto e responsabilità, passim.*

[26] G. OPPO, *Sul consenso dell'interessato*, in *Trattamento dei dati e tutela della persona*, a cura di Cuffaro, Ricciuto e Zeno Zencovich, Milano, 1998, p. 230.

[27] G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 336 ss.

[28] Si segnalano sul punto le recenti Direttiva 2019/770/UE relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali e la dir. 2019/2161/UE che aggiorna le Direttive 93/13/CEE (clausole abusive nei contratti con i consumatori), 98/6 (indicazione dei prezzi sui prodotti di consumo), 2005/29 (relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno) e 2011/83 (in materia di protezione dei consumatori nei contratti a distanza) per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori. A titolo esemplificativo, successivamente all'aggiornamento operato da Direttiva 2161/2019/UE, la Direttiva 83/2011/UE si applicherà non solo, come avviene, ora ai contratti di servizi, compresi i contratti di servizi digitali, che prevedono che il consumatore paghi o si impegni a pagare un prezzo ma anche in relazione ai contratti per la fornitura di contenuto digitale online indipendentemente dal fatto che il consumatore paghi un prezzo o fornisca dati personali a titolo di corrispettivo.

[29] V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, cit., p. 95 ss.; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella riscostruzione del fenomeno*, in *Dir. inform.*, 2018, p. 689 ss.; C. PERLINGIERI, *Profili civilistici dei social network*, Napoli, 2014; P. GIUGGIOLI, *Tutela della* privacy *e consumatore*, in *Privacy digitale*, a cura di Tosi, Milano, 2019, p. 263 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali, cit.;* e da ultimo *T.M.* UBERTAZZI *Ripensando alla revoca del consenso nella prospettiva funzionale della privacy*, in questa *Rivista, 2022,* p. 27 ss.; E. BATTELLI, *Negoziabilità dei dati personali e modelli di valorizzazione economia,* in *Riv. di Diritto dell'impresa,* 2022, p. 21 ss.

erroneamente, l'esplicito dato testuale del citato regolamento europeo lasciando tralatiziamente prevalere, anche in relazione al mero attributo immateriale della personalità, la natura di diritto fondamentale della personalità, perseverando nel ritenere il dato personale oggetto improprio di atti dispositivi e così disattendendo il principio di bilanciamento con la libera circolazione del dato personale[30].

Senza dimenticare, infine, che il GDPR non interferisce certo sul piano contrattuale non essendo questa la finalità del legislatore europeo che infatti non viene mai richiamata tra gli scopi della normativa in parola: tale ambito normativo rimane, invero, ascrivibile esclusivamente all'autonomia dei singoli Stati membri.

5. Patrimonializzazione e monetizzazione dei dati personali alla luce del nuovo art. 135 octies Codice del Consumo.

La rilevanza economica dei dati personali non si riduce certo alle generalità anagrafiche della persona, anzi.

Comprende pervero il ben più significativo e rilevante valore commerciale offerto dall'analisi massiva dei *metadati* generati non solo dei *motori di ricerca* ma soprattutto dei dispositivi digitali utilizzati *smartphone, digital assistant* e *wearables* per citare i casi più emblematici, vere e proprie memorie digitali della nostra vita privata e professionale.

Nella prassi mercatoria digitale emergono due modelli di scambio correlati ai dati personali.

Un primo schema negoziale, molto diffuso, è basato sull'equazione servizi e contenuti digitali a fronte della controprestazione di dati personali del fruitore del servizio anche oltre quanto strettamente necessario all'esecuzione.

Un secondo schema negoziale meno ricorrente nella prassi ma non certo secondario prevede il consenso contrattuale al trattamento a fronte della monetizzazione dei dati e registra dunque l'ulteriore evoluzione del mercato dei *data broker*.

Un modello di circolazione dei dati personali fondati su un contratto in cui l'oggetto unico è proprio l'utilizzo dei dati personali a fronte di un corrispettivo liquidato al soggetto interessato dal titolare del trattamento.

Nel primo caso i dati personali sono controprestazione di altri servizi digitali; nel secondo caso i dati personali sono oggetto del contratto di trattamento a titolo oneroso per il titolare del trattamento e non dell'interessato dal trattamento che viene per tale ragione remunerato.

Si registra in merito, almeno con riferimento al primo schema negoziale, un punto di non ritorno normativo relativamente alla patrimonializzazione dei dati e alla circolazione contrattuale dei dati stessi in quanto controprestazione contrattuale vera e propria nei contratti di fornitura di contenuti e servizi digitali: non più dunque dati personali richiesti e trattati solo perché necessari per l'esecuzione di contratto, caratterizzati da un mero rilievo strumentale ed estranei al sinallagma contrattuale.

[30] Si vedano in tal senso: V. RICCIUTO, *L'equivoco della privacy,* Napoli, 2022, *passim.*

Si tratta dell'ormai ben noto D.Lgs. 4 novembre 2021, n.173 di recepimento della Direttiva UE 2019/770 inerente la fornitura di contenuti e servizi digitali modifica che aggiorna il *Codice del Consumo* (d.lgs. 206/2005) introducendo il nuovo capo I-bis *Dei contratti di fornitura di contenuto digitale e servizi digitali.*

La disciplina consumeristica italiana si arricchisce così delle tutele previste dalla Dir.UE 2019/770 per i contratti di fornitura di contenuti o servizi digitali: in particolare, sono previsti specifici obblighi del professionista, responsabilità e rimedi a favore del consumatore per la mancata fornitura o per i difetti di conformità che non è possibile approfondire in questa sede.

Corre l'obbligo di richiamare innanzitutto, ai sensi dei commi 3 e 4 de nuovo articolo 135 *octies* del Codice del Consumo che le disposizioni del Capo I *bis* si applicano a due diverse ipotesi di accordo:

- a qualsiasi contratto in cui il professionista fornisce, o si obbliga a fornire, un contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si obbliga a corrispondere un prezzo;
- al caso in cui il professionista fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o *si obbliga* a fornire dati personali al professionista, quando tali dati non sono trattati dal professionista esclusivamente per l'esecuzione del contratto ma costituiscono essi stessi oggetto di un autonomo contratto di trattamento dati personali.

Si è già dato conto del dibattito dottrinale in ordine alla seconda ipotesi in quanto essa pone dei rilevanti problemi di coordinamento con la disciplina per la protezione dei dati personali delineata dal GDPR.

Emerge la volontà del legislatore europeo, pur con tutte le ambiguità lessicali del caso, non tanto di rendere i dati personali assimilabili a un mezzo di pagamento in senso stretto, cosa che certamente non è, ma di riconoscere la rilevanza patrimoniale della controprestazione consistente nella comunicazione dei propri dati personali con relativo consenso al trattamento per finalità ulteriori rispetto a quelle dell'esecuzione del contratto stesso.

Quanto detto al fine di garantire anche a queste situazioni diffusissime nella pratica dei mercati digitali, alla base del successo globale delle *big tech* della *silicon valley*, le ulteriori tutele consumeristiche rafforzate assicurate ai contratti di fornitura di contenuti e servizi digitali integrative dei rimedi generali già assicurati dal GDPR.

Per completezza si segnala il considerando 24 della dir. (UE) 2019/770 secondo cui: *"La presente direttiva dovrebbe pertanto applicarsi ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a fornire, dati personali".*

Inoltre *"La presente direttiva dovrebbe altresì applicarsi nel caso in cui il consumatore acconsenta a che il materiale che caricherà e che contiene dati personali, come fotografie o post, sia trattato a fini commerciali dall'operatore economico. Gli Stati membri dovrebbero tuttavia mantenere la facoltà di decidere in merito al soddisfacimento dei requisiti in materia di formazione, esistenza e validità di un contratto a norma del diritto nazionale".*

Si evince dal predetto considerando che sul tema dell'utilizzo dei dati personali a titolo di controprestazione è stato lasciato un margine

di discrezionalità agli Stati membri**:** per disciplinare il contratto di utilizzo dei dati in base alle specifiche regole ordinamentali dei rispettivi Stati membri.

L'Italia ha, purtroppo, perso un'occasione per esercitare la propria autonomia legislativa e chiarire il tema controverso denso di implicazioni giuridiche, non solo civilistiche.

Su questo aspetto il legislatore si è limitato a una mera, scolastica, trasposizione della lettera della Direttiva nella normativa di recepimento interno, lasciando quindi aperta la questione in ordine ad ammissibilità e limiti a tacere dell'omesso raccordo di tale contratto atipico - avente ad oggetto proprio il trattamento di dati personali che entrano a far parte del sinallagma contrattuale - con la disciplina contrattuale generale del Codice Civile e con i rimedi consumeristici previsti dalla stessa normativa appena introdotta e infine con il GDPR.

Limitandosi a statuire con norma, scontata per non dire superflua, al comma 6 dell'articolo 135-novies Codice del Consumo la prevalenza del GDPR in caso di conflitto, sulle disposizioni del nuovo Capo I-bis: a parte questo opinabile riferimento espresso, la controprestazione con dati personali del consumatore non è oggetto di ulteriore considerazione normativa.

L'art.135-noviesdecies del Codice del Consumo al comma 3 si limita, infatti, didascalicamente ad affermare che "*Per quanto riguarda i dati personali del consumatore, il professionista è tenuto a rispettare gli obblighi derivanti dal regolamento (UE) 2016/679 nonché dal d.lgs. 101/2018***".**

Ma quanto affermato era già logica conseguenza della prevalenza, già affermata, della normativa del GDPR. Rimangono, invece, a carico dell'interprete problemi irrisolti dal d.lgs**.** 173/2021 relativi al contratto di utilizzo dei dati personali

Si segnalano per rilevanza *ex multis*: il problema dell'applicabilità anche ai contratti di utilizzo dei dati personali del diritto alla congrua riduzione del prezzo in caso di difetto di conformità, della sorte dei dati personali forniti dall'utente a fronte della risoluzione del contratto, a tacere del problema controverso, allo stato irrisolto, della revocabilità, limitata o illimitata, del consenso al trattamento dei dati stessi.

6. Dati personali e contratto: una convergenza rimediale opportuna.

Alla luce di quanto sopra osservato si può affermare che nei mercati digitali rileva un doppio fenomeno contrattuale correlato all'utilizzo dei dati personali:

- da un lato, secondo lo schema di *asimmetria ordinaria* fornitore forte e contraente debole, l'emersione della funzione di controprestazione del consenso al trattamento dei propri dati a fronte di servizi digitali resi dal prestatore online come segnalato anche nella recente normativa europea (c.d. *patrimonializzazione)*;

- dall'altro la remunerazione dell'interessato, secondo lo schema di *asimmetria inversa "*fornitore" dei dati personali debole e contrente forte-titolare del trattamento, a fronte dello sfruttamento dei propri dati personali per finalità economiche da parte dei *Big Tech* (c.d. *monetizzazione).*

Alla luce di quanto sopra osservato risulta, dunque, evidente che la lettura

tradizionalista restrittiva in ordine alla circolazione contrattuale dei dati personali sia frutto, come già segnalato, di un equivoco interpretativo che vede sovrapporsi e prevalere sempre la tutela della persona rispetto alla circolazione dei dati personali[31].

Ma così non è.

Fermo restando il limite inviolabile della dignità personale - riconosciuto dall'art. 2 della nostra *Costituzione* oltre che dall'art. 1 della *Carta dei diritti fondamentali dell'Unione Europea* - e dell'*asservimento definitivo* dei dati personali - che come ci ricordava Stefano Rodotà, è da considerarsi inammissibile - nulla osta alla compatibilità dogmatica, in ossequio a lettura moderna attenta al dato sistematico complessivo e ai principi di bilanciamento emergenti dalla normativa europea introdotta dal GDPR, tra persona, dati personali e circolazione contrattuale[32].

Sono compatibili e coesistono da un lato il potere unilaterale di autodeterminazione informativa della persona in relazione al consenso autorizzatorio e dall'altro il potere contrattuale in relazione al consenso contrattuale rilevante in base alle normative dei singoli Stati membri: il GDPR non elide né interferisce con la disciplina del consenso contrattuale, né potrebbe farlo essendo tale materia estranea all'ambito di applicazione del regolamento stesso.

Consenso autorizzatorio – libero, specifico, informato e inequivocabile (art. 4 GDPR) – che rileva dunque esclusivamente quando il trattamento dei dati personali non risulta fondato giuridicamente su un rapporto contrattuale ma prescinde da esso (art. 6.1, lett. a GDPR).

Consenso contrattuale - altrettanto, libero, trasparente ed informato - nel caso in cui invece il trattamento dei dati personali necessario per l'esecuzione dello stesso o di attività precontrattuali su richiesta dell'interessato oppure sia oggetto del contratto stesso (art. 6.1, lett. b GDPR).

Consenso contrattuale che risulta quindi assorbente rispetto al consenso autorizzatorio quando è proprio il trattamento dati personali ad essere oggetto del contratto o della necessaria esecuzione dello stesso.

Alla luce di quanto sopra evidenziato si tratta solo di un contrasto, apparente, tra tutela della persona e dei diritti fondamentali della personalità, che non s'intendono certo mettere in discussione, e circolazione contrattuale dei dati personali.

Attività quest'ultima che, come si è già avuto modo di rilevare, non solo non è vietata ma è al contrario espressamente tutelata dall'art.1.1 e 1.3 GDPR: d'altra parte anche la giurisprudenza più recente, pervero, progressivamente valorizza e ammette la dimensione patrimoniale e contrattuale dell'utilizzo dei dati personali[33].

---

[31] V. RICCIUTO, *L'equivoco della privacy,* cit., *passim.*

[32] Così S. RODOTÀ, *Conclusioni*, in *Trattamento dei dati e tutela della persona*, a cura di Cuffaro-Ricciuto-Zeno Zencovich, Milano, 1999, 308.

[33] Con la significativa sentenza n. 2631 del 29 marzo 2021, il Consiglio di Stato ha respinto il ricorso presentato dalla società Facebook Ireland Limited avverso il provvedimento dell'Autorità garante della concorrenza e del mercato (AGCM), adottato il 29 novembre 2018 (AGCM provv. n. 27432 del 29 novembre 2018) già impugnato di fronte al TAR Lazio TAR Lazio, sez. I, 10 gennaio 2020, n. 260. Due punti della sentenza del CdS meritano segnalazione. Il primo riguarda il dibattuto tema dello sfruttamento dei dati personali per finalità commerciali nell'ambito di un servizio digitale. Si chiarisce opportunamente che, anche a prescindere dalla espressa qualificazione del trattamento dati in termini di corrispettivo del servizio,

La circolazione contrattuale dei dati personali pur ammissibile non è, tuttavia, da considerarsi affare strettamente privato delle parti ma risulta soggetto alla stringente *conformazione contrattuale* del GDPR oltre che alla regolazione pubblica assicurata dall'attenta vigilanza del Garante per la protezione dei dati personali.

In questa prospettiva interpretativa rigorosa, pare potersi, pertanto, ammettere e disciplinare compiutamente il fenomeno dello sfruttamento economico dei dati personali si badi bene, sempre, *temporaneo* e *non esclusivo*.

Tale operazione contrattuale di "sfruttamento" economico dei dati personali potrà ben essere realizzata ricorrendo allo strumento di libertà e giustizia, che è il *contratto conformato*[34]*,* espressione di autonomìa contrattuale non libera bensì *autonomìa conformata* soggetta ai principi e precetti regolatori inderogabili del GDPR oltre che alla normativa protettiva consumeristica applicabile a protezione del soggetto debole, ossia colui che conferisce i dati personali, meritevole di protezione rispetto agli abusi contrattuali del contraente forte in ragione della strutturale asimmetria contrattuale peculiare del rapporto di trattamento dati personali.

In tale prospettiva merita, dunque, protezione rimediale rafforzata non solo il soggetto debole che consente l'utilizzo dei propri dati quale "corrispettivo" a fronte di beni o servizi forniti dal titolare del trattamento ma anche il soggetto interessato dal trattamento che in fattispecie di asimmetria inversa viene remunerato proprio per tale "cessione" temporanea e non esclusiva che diviene esplicitamente oggetto del rapporto contrattuale.

Pare, infatti, doveroso assicurare giusta protezione rafforzata consumeristica, in ossequio a lettura assiologica costituzionalmente orientata, oltre il formalismo definitorio[35], anche quando il soggetto debole interessato non sia strettamente qualificabile come *consumatore* fruitore di beni e servizi ma semmai "fornitore" di propri dati personali al titolare del trattamento e pur sempre meritevole di beneficiare dei rimedi protettivi consumeristici individuali e metaindividuali: questi ultimi più che mai necessari per la protezione del soggetto debole *persona-interessato-consumatore* nella dimensione strutturalmente asimmetrica del capitalismo della sorveglianza

---

l'attività del fornitore risulta soggetto all'ambito di applicabilità della disciplina europea sulla protezione dei dati personali oltre che dalla disciplina protettiva contrattuale consumeristica. Il secondo riguarda il tema correlato della solo apparente gratuità del servizio digitale nel caso di consenso all'utilizzo dei propri dati personali. Se il fornitore di un servizio sfrutta commercialmente i dati degli utenti che tale servizio digitale utilizzano – anche a prescindere alla qualificazione formale in termini di corrispettivo del servizio – nella sostanza il servizio non può essere presentato al pubblico come gratuito perché tale in effetti non è. Si vedano inoltre AGCM 9 novembre 2021, n. 298; TAR Lazio 10 gennaio 2020, n. 260 e 261 con nota di C. SOLINAS, *Circolazione dei dati, onerosità del contratto e pratiche commerciali scorrette, in Giurisprudenza italiana; cui adde* SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali,* Bari, 2022; e *da ultimo* MATERA, *Patrimonializzazione dei dati personali e pratiche commerciali scorrette,* in *Tecnologie e diritto,* 2022, 155 ss.

[34] G. BERTI DE MARINIS, *Contratti dei mercati regolamentati: norme imperative e conformazione,* Napoli, 2019; C. SOLINAS, *Il contratto amministrato. La conformazione dell'operazione economica agli interessi generali,* Napoli, 2018.

[35] Sulla forza espansiva e sulla giusta flessibilità dei rimedi protettivi consumeristici applicabili a tutte le situazioni contrattuali asimmetriche in cui il soggetto debole risulti meritevole di tutela si vedano P. PERLINGIERI, *La tutela del consumatore nella Costituzione e nel Trattato di Amsterdam, in* P. PERLINGIERI-E. CATERINI (a cura di), *Il diritto dei consumi*, I, Napoli, 2004 13 ss.; e G. ALPA, *Le stagioni del contratto,* Bologna, 2012, 143.

digitale[36].

7. L'emersione del contratto di utilizzo dei dati personali e limiti all'autonomia delle parti: un nuovo contratto atipico conformato e regolato.

In ogni caso, a prescindere dai dubbi interpretativi e dagli aspetti problematici richiamati *supra,* è ormai evidente a tutti la progressiva, quanto inarrestabile, consumerizzazione dell'interessato dal trattamento e la patrimonializzazione dei dati personali.

In linea con lo sdoppiamento peculiare dei diritti della personalità immateriali si registra la triplice dimensione giuridica di *persona-interessato-consumatore*.

Solo almeno tre gli indizi normativi evocabili allo scopo di teorizzare la liceità del contratto di utilizzo dei dati personali altrui, fermo restando l'osservanza dei precetti conformativi del GDPR e il limite invalicabile della dignità personale.

Il primo indizio normativo: la normativa europea riconosce espressamente la libera circolazione dei dati personali nell'Unione Europea del *digital single market* e che la stessa "non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali" (art.1.3 GDPR).

Il secondo: si ricomprende espressamente tra le condizioni di liceità il *consenso contrattuale* (art. 6.1 lett. b GDPR) in alternativa al *consenso autorizzatorio* dell'interessato dal trattamento (art. 6.1 lett. a GDPR).

Il terzo, non certo per importanza, quando ammette che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati non necessari così ammettendo implicitamente che sia ammissibile ipotizzarsi la fattispecie contrattuale in cui il consenso sia invece necessario per l'esecuzione del contratto senza escludere espressamente che l'oggetto del contratto abbia ad oggetto proprio il trattamento dei dati personali in se e per sé considerato (art. 7.4 GDPR).

Come, invero, accade quando è proprio il trattamento e utilizzo dei dati personali altrui ad essere esclusivo oggetto di un contratto di utilizzo e trattamento dei dati personali – impropriamente definito di "cessione" dei dati personali in ossequio a una logica esclusivamente proprietaria che, tuttavia, non rende la complessità del fenomeno – a fronte di una remunerazione da parte del titolare del trattamento.

Si ammette, quindi, non solo il caso in cui il consenso al trattamento dei dati sia considerato il "corrispettivo" di un servizio fornito ma anche il suo opposto ossia il caso diverso e speculare in cui il consenso all'utilizzo dei propri dati personali sia oggetto del contratto stesso e che per tale ragione l'interessato dal trattamento dei dati venga remunerato dal Titolare del trattamento.

Si tratta dunque non di ignorare ma piuttosto di qualificare correttamente e disciplinare il ben noto fenomeno contrattuale della "cessione" del diritto di

[36] Nel senso di una progressiva convergenza e in ordine all'applicabilità, in prospettiva di tutela collettiva, della normativa consumeristica all'interessato dal trattamento dati personali si veda la già citata sentenza della Corte di Giustizia UE del 28 aprile 2022 relativa alla causa C319/20.

sfruttamento economico, temporaneo e non esclusivo, dei propri dati personali condizionata all'osservanza del GDPR[37].

Sia con riferimento al caso assai diffuso dello scambio servizi digitali-dati personali, parzialmente regolato nel Codice del Consumo, come pure al caso speculare di asimmetria rovesciata in cui il trattamento dei dati personali altrui è l'unico oggetto del contratto e il consenso dell'interessato viene quindi remunerato dal titolare soggetto forte destinatario della prestazione, non fornitore, con un corrispettivo pecuniario.

In questo singolare caso, ignorato dal Codice del Consumo, il contraente che presta il consenso al trattamento dei propri dati a fronte di un corrispettivo pur non essendo *consumatore in senso formale* pare, comunque, meritevole di protezione in quanto pur sempre soggetto debole del rapporto in senso sotanziale in ossequio a lettura assiologica costituzionalmente orientata oltre gli angusti limiti formali della tutela consumeristica[38].

Un'occasione mancata, si ribadisce, da parte del legislatore italiano per fare chiarezza – in occasione del recepimento della Direttiva UE 2019/770 - su questioni interpretative complesse, fra cui si segnala anche quella dello scambio di servizi analogici tradizionali contro dati personali come pure della revoca del consenso, che avrebbe potuto essere colta tipizzando il contratto di trattamento dei dati personali che, invece, allo stato, rimane consegnato, a prassi mercatorie incontrollate e poco trasparenti[39].

Non limitarsi a far emergere lo scambio di servizi digitali contro dati personali ma riconoscere e disciplinare espressamente il fenomeno contrattuale dello scambio di beni e servizi tradizionali contro dati personali e soprattutto del contratto di trattamento dati.

Ossia di quel contratto *atipico* avente ad oggetto specifico e caratterizzante proprio il trattamento dei dati personali: un tale intervento normativo avrebbe significato un giusto rafforzamento rimediale della posizione debole dell'interessato dal trattamento.

Contratto di "cessione dei dati" che – ferma restando la necessità di superare positivamente il filtro civilistico del giudizio di meritevolezza ex art. 1322 secondo comma c.c. - certamente si caratterizza per essere sottratto alla libertà contrattuale piena delle parti ed essere assoggettato alla libertà contrattuale conformata al GDPR e vigilata dal *Garante per la protezione dei dati*

---

[37] P. GALLO, *Il consenso al trattamento dei dati personali come prestazione,* in *Riv. Dir. Civ.,* 2022, pp. 1054 ss.; T.M. UBERTAZZI, *Ripensando alla revoca del consenso nella prospettiva funzjonale della privacy,* in *Contratto e impresa,* 2022, pp. 27 ss.; e da ultimo S. ORLANDO, *Per un sindacato di liceità del consenso,* in *Persona e mercato,* 2022, pp. 527 ss.

[38] Sulla forza espansiva e sulla giusta flessibilità dei rimedi protettivi consumeristici applicabili a tutte le situazioni contrattuali asimmetriche in cui il soggetto debole risulti meritevole di tutela si vedano P. PERLINGIERI, *La tutela del consumatore nella Costituzione e nel Trattato di Amsterdam, in* P. PERLINGIERI-E. CATERINI (a cura di), *Il diritto dei consumi*, I, Napoli, 2004 13 ss.; e G. ALPA, *Le stagioni del contratto,* Bologna, 2012, 143.

[39] E. TOSI, *Circolazione contrattuale dei dati personali tra contratto e responsabilità, op. cit.,* pp. 78 ss.; E.TOSI, *Diritto Privato delle Nuove Tecnologie Digitali. Riservatezza. Contratto, riservatezza, responsabilità tra persona e mercato, cit.*; *cui adde ID., Privacy Digitale,* a cura di Tosi, cit.; ID. *Unlawful Data Processing Prevention and Strict Liability Regime Under EU GDPR, in Italina Law Journal, 2021, p. 873 ss.; Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, *cit.; I Poteri privati delle piattaforme digitali e le nuove frontiere della privacy,* a cura di Stanzione, Torino, 2022; V*alore economico dei dati tra diritto pubblico e diritto privato,* a cura di Colapietro e Simoncini, Torino, 2022, *passim*. Sul tema specifico della revoca del consenso nei contratti aventi ad oggetto il trattamento dei dati personali: T.M. UBERTAZZI, *Ripensando alla revoca del consenso nella prospettiva funzionale della privacy,* in *Contratto e impresa,* 2022, 27 ss.

personali

In tale prospettiva il contratto oltre che meritevole di tutela ai sensi dell'art. 1322 comma 2 c.c. dovrà pertanto essere conformato ai precetti del GDPR fra cui in particolare al trattamento per *finalità determinate, esplicite e soprattutto legittime (Art.5.1, lett. b GDPR).*

Si tratta, ad avviso di chi scrive, di un *contratto atipico,* sulla falsariga del modello di *licenza d'uso temporanea* affermatosi nel settore dell'utilizzo dei contenuti digitali e altri beni immateriali, pure sdoppiati tra dimensione personale e patrimoniale del diritto.

Contratto atipico conformato e regolamentato: conformato ai precetti inderogabili del GDPR a cui le parti debbono necessariamente attenersi nella stesura delle regole contrattuali e regolamentato dall'autorità di controllo competente, ossia il Garante per la protezione dei dati personali.

L'operazione di "sfruttamento" economico dei dati personali è espressione, almeno in linea teorica, di legittima autonomia contrattuale, compatibile con il GDPR, ferma restando la necessità di verificare, caso per caso, in concreto la meritevolezza degli interessi perseguiti dal contraente forte al fine di proteggere il contraente debole dagli abusi contrattuali.

Tale funzione protettiva potrà essere adeguatamente realizzata ricorrendo allo strumento di libertà e giustizia, che è il *contratto conformato*[40]*,* espressione di autonomìa contrattuale non libera bensì *autonomìa conformata* soggetta ai principi e precetti regolatori inderogabili del GDPR oltre che alla normativa protettiva consumeristica applicabile a protezione del soggetto debole, ossia colui che conferisce i dati personali, meritevole di protezione rispetto agli abusi contrattuali del contraente forte in ragione della strutturale asimmetria contrattuale peculiare del rapporto di trattamento dati personali.

La circolazione contrattuale dei dati personali pur ammissibile non è, infatti, da considerarsi affare strettamente privato delle parti ma risulta soggetto alla stringente *conformazione contrattuale* del GDPR oltre che alla regolazione pubblica assicurata dal Garante per la protezione dei dati personali.

In questa prospettiva interpretativa rigorosa, pare potersi, pertanto, ammettere e disciplinare compiutamente il fenomeno dello sfruttamento economico dei dati personali, sempre, *temporaneo* e *non esclusivo,* e funzionale al perseguimento di finalità di trattamento legittime e interessi contrattuali meritevoli di tutela.

In conclusione, a composizione dell'ossimoro apparente tra dati personali e contratto, si apre la strada a una condivisibile lettura moderna del fenomeno contrattuale che consente giustamente, in conformità ai precetti costituzionali e alla *Carta dei diritti fondamentali* UE, un *surplus* rimediale a tutela della persona e non un *deficit* protettivo.

Non solo soccorrono, dunque, i rimedi offerti dal GDPR ma anche tutele e rimedi offerti dalla convergenza protettiva rafforzata e integrata del Codice del Consumo.

Rimedi e tutele che concorrono in ultima istanza alla protezione della dignità della *persona-interessato-consumatore* non solo in prospettiva

[40] G. Berti De Marinis, *Contratti dei mercati regolamentati: norme imperative e conformazione,* Napoli, 2019; C. Solinas, *Il contratto amministrato. La conformazione dell'operazione economica agli interessi generali,* Napoli, 2018.

individualistica, ma collettiva [41], non solo in dimensione strettamente privatistica ma regolatoria, del contratto e di riflesso dei mercati.

[41] Nel senso di una progressiva convergenza e in ordine all'applicabilità, in prospettiva di tutela collettiva, della normativa consumeristica all'interessato dal trattamento dati personali si veda la già citata sentenza della Corte di Giustizia UE del 28 aprile 2022 relativa alla causa C319/20.

Borroni A, Zambardino F, 'Distributed Ledger Technologies (DLTs) and right to health: the impact of blockchain in the healthcare sector' (2023) 2 EJPLT, 93 - 110.
DOI: https://doi.org/10.57230/EJPLT232ABFZ

EJPLT
ISSN 2704-8012



Distributed Ledger Technologies (DLTs) and right to health: the impact of blockchain in the healthcare sector

Distributed Ledger Technologies (DLTs) e diritto alla salute: l'impatto della blockchain nel settore sanitario

ANDREA BORRONI
Associate Professor of Comparative Law
University of Campania Luigi Vanvitelli

FABIO ZAMBARDINO
Post-doctoral fellow
University of Campania Luigi Vanvitelli

Abstract

The aim of this contribution is to understand whether and how the blockchain technology can be used in the health sector, analyzing the ways in which its incorporation into the management of health data infrastructure might have the potential to create a more efficient national healthcare system.

L'obiettivo del presente contributo è quello di analizzare se e come la tecnologia blockchain possa essere utilizzata nel settore sanitario, verificando le modalità in cui la sua incorporazione nella gestione dell'infrastruttura dei dati sanitari potrebbe avere il potenziale per creare un sistema sanitario nazionale più efficiente.

© The author(s) 2023, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Blockchain; Healthcare; Electronic Health Record; Data protection; Telemedicine.

Summary: Introduction – 1. The main features of blockchain technology. – 2. How blockchain fits into the healthcare sector. – 3. Different types of blockchain. – 4. Health protection and data protection. – 5. Blockchain and telemedicine. – Conclusive remarks.

Introduction.

The use of new technologies in the healthcare sector has only recently started to develop, more for medical-diagnostic use than for the purpose of facilitating healthcare organisation *stricto sensu*.[1]

The prompt advent of the Internet of things (IoT) paradigm has introduced several innovative elements, generating major improvements in terms of, *inter alia*, electronic medical records, data sharing on the production and circulation of drugs, in relation to insurance information, and in terms of facilitating remote assistance.[2]

From a strictly legal point of view, the ability of the existing rules to reshape themselves to intercept the reorganisation of the law caused by the

* Even though the article is the product of common critical analysis and considerations, Andrea Borroni authored paragraphs: 3, 6, 7 and Fabio Zambardino authored paragraphs: 1, 2, 4, 5.

[1] The introduction of digitisation in the health sector has its origins in the reform of the public administration, conceived since the times of the 1999 Bassanini reforms, but at that stage it was soon abandoned due to the difficulty of the public administration in accepting such significant transformations, to the absence of a suitable network and digitisation of the administration, and, in any case, to the backwardness of the state and regional administrative context incapable of accepting such innovations. For a reconstruction of digitalization in public administration see G Duni, *L'Amministrazione digitale* (Giuffrè 2008); F Bassanini, 'Twenty years of administrative reformsin Italy' (2009) 3 Review of Economic Conditions in Italy, 369 ff; E Carloni, 'L'amministrazione aperta. Regole e limiti dell'open Government' (2014) Orizzonti di Diritto Commerciale; F Martines, 'La digitalizzazione della pubblica amministrazione' (2018) 2 Medialaws; R Cavallo Perin, D U Galetta (ed.), *Il diritto dell'Amministrazione Pubblica digitale* (Giappichelli 2020). In 2005, with the approval of the Digital Administration Code, a start was then made on giving shape to this project, in particular in the light of articles 43 and 44 where it is stipulated that any document, which by law or regulation must be stored, may be reproduced and stored on computer support, if the relevant procedures are carried out in such a way as to guarantee conformity with the original documents and comply with the Guidelines, but then leaving the possibility of maintaining storage in paper form. E Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (2022) 4 Federalismi, 214. It was only in 2012 that these objectives were transformed into concrete regulations, and in particular with Article 47-bis of Decree-Law No. 5/2012, converted, with amendments, by Law No. 3 of 4 April 2012), which speaks of digital healthcare and with the approval of Decree-Law No. 179 (later converted, with amendments, by Law No. 221 of 17 December 2012), which more explicitly dematerialises medical records, which no longer need to be made into a paper document and signed by healthcare personnel, even if they were already drawn up by the health authorities. 221 of 17 December 2012), which more explicitly dematerialised the medical record, which in fact no longer needs to be turned into a paper document and signed by the healthcare personnel, even if it is already in the so-called computerised medical record, but is limited to being in electronic format in all respects. *Ibid.*

[2] See for a general overview M Durante, U Pagallo (eds.), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, (Giappichelli 2013).

involvement of innovative technologies is an indispensable condition for the full affirmation of rights in the encounter between health and technological innovation and thus, in the final analysis, for the concrete implementation of the constitutional guarantee of health as a fundamental right of the individual and interest of the community.[3]

In particular, an important role can be played by the blockchain that, due to its operational versatility, makes it possible to shape a distributed database for the management of common transactions, in which traceability and unchangeability are guaranteed; furthermore, the executive continuity of the system is ensured by the union of widespread control (peer to peer), with cryptographic techniques.[4]

Given the premises, this paper aims to provide, firstly, a brief examination of the functioning of the distributed ledger system and, secondly, to investigate the actual possibility of finding a point of balance between the need to protect the privacy of the subject concerned and that of health protection, in order to favour a concrete evaluation of the suitability of personal data protection to act as an extreme boundary to the right to health.[5]

1. The main features of blockchain technology.

In terms of definition, the blockchain can be considered a public ledger containing the history of all transactions and/or operations entered into it.

Its structure consists of a concatenated list of data, into which the nodes of the network – *i.e.,* computers connected to the ledger – enter blocks of information according to the rules of the implementation system.[6]

A chronological digital ledger, therefore, whose contents can be verified by any device with an internet connection. Each blockchain is then encrypted and

[3] F Aperio Bella, 'L'accesso alle tecnologie innovative nel settore salute tra universalità e limiti organizzativi (con una postilla sull'emergenza sanitaria)' (2020) 1, PERS. AMM., 220. See also G Pascuzzi, U Izzo, 'Le problematiche giuridiche connesse all'utilizzo delle nuove tecnologie in sanità' (2012), psychiatryonline.it, 155-163.

[4] M Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (2020) 21, Federalismi, 173.

[5] Two principles, those enunciated above, which are certainly not opposed, but rather complementary, and which constitute the expression, with different nuances, of the common value of human dignity and personality referred to in Article 2 of the Constitution. On the "open" nature of the enumeration contained in Article 2 of the Constitution, see A Barbera, 'Commento all'art. 2 della Costituzione', in G Branca (ed.), *Commentario della Costituzione italiana* (1995) Zanichelli; P Rescigno, 'Personalità (diritti della)', *Enciclopedia Giuridica* XXIII (1990) 1 ff; V Zeno Zencovich, 'Personalità (diritti della)', *Digesto delle Discipline Privatistiche* XIII (1995) 453 ff. See also E Frosini, 'Tecnologie e libertà costituzionali, in G Comandé, G Ponzalli (eds.), *Scienza e diritto nel prisma del diritto comparato* (Giappichelli 2004), 189, who, still on the subject of the relationship between technology and privacy, states how new technological discoveries have represented and continue to represent a development of freedoms; indeed, freedoms have been able to greatly increase and expand towards new frontiers of human action precisely because of technological progress.

[6] A Wright, P De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia (Panthéon-Assas 2015) 6.

organised into groups of smaller transactions called blocks.[7]

The content of this database is verified through a mechanism that requires the authorisation of all participants in the blockchain since, once information has been entered into the system, it cannot be deleted unless 'changes are approved by the majority of the computing power of the entire blockchain'.[8]

Moreover, a copy of the blockchain is stored on all the computers in the network that are periodically synchronised to ensure that all users have the same shared database.[9]

The essential element of such a system is decentralisation, which describes the process of diversification and dispersal of power from a central authority,[10] the basis of which is to be found in the creation of a *sui generis* network through which transactions can be carried out in a more secure and flexible manner.[11]

This, in fact, allows the blockchain greater resistance to attacks since, if one or more nodes stop functioning, however, "trust" can be maintained by relying on the other nodes.

Unlike centralised systems, where the administrator acts as the pivot point for each user instance and where storage is carried out at a single level, with a consequent risk of data loss,[12] in distributed structures, each node acts as a depository of a copy of the registry and all changes that are made are subject to the approval of the entire community of nodes, based on (computer) consensus rules established in the algorithm.[13]

Finally, a further strong point is outlined by the guarantee of information transparency since users have a fully verifiable register at their disposal.[14]

2. How blockchain fits into the healthcare sector.

The use of Distributed Ledger Technologies, such as blockchain, has extended from the cryptocurrency market to other fields, including, for instance, the privacy sector.[15]

---

[7] A Borroni, 'Blockchain: Uses and Potential Value', in A Borroni, *Legal Perspective on Blockchain Theory, Outcomes, and Outlooks*, (ESI 2019) 5.

[8] *Ibid.*

[9] Wright, De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (n 6) 6-8.

[10] R Böhme and others, 'Bitcoin: Economics, Technology, and Governance' (2014) 29 J. ECON. PERSP., 219-220.

[11] M Abramowicz, 'Cryptocurrency-Based Law', in *GWU Law School Public Law Research Paper* (2015) 6-7.

[12] M Giuliano, 'La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio' (2019) DIR. INFORM., 996.

[13] Borroni, 'Blockchain: Uses and Potential Value' (n 7) 6-7.

[14] Abramowicz, 'Cryptocurrency-Based Law' (n 11) 9. A level of transparency that, according to the author, should ensure a higher level of adoption of blockchain technology. See, on the topic of transparency, Iorio, *A Modern Approach to Global Tax Transparency and Beneficial Ownership Registers: Forget Sunlight, Is Blockchain the Best Disinfectant?* (New York Law School 2020); PK Medhi, *Role of Blockchain Enabled Transparency in Risk Management and Sustainability of the Complex Global Supply Chains*, (Bennett University 2019).

[15] For an analysis of the different use cases of the blockchain technology, be permitted a reference to Borroni, 'Blockchain: Uses and Potential Value' (n 7) 7.

In particular, the need for decentralisation lies in the growing concern of users about the loss of control over their personal data stored on the Internet.[16]

In this respect, the very structure of blockchain technology would allow data privacy to be preserved; however, such architectures can sometimes prove vulnerable to metadata analysis. Consequently, if not properly designed, 'decentralized infrastructures intended to promote individual privacy and autonomy might turn out to be much more vulnerable to governmental or corporate surveillance than their centralized counterparts'.[17]

Given the technological substratum discussed in the previous section, the reason for the interest of researchers from a wide range of fields in the potential of DLTs in terms of data management is inherent in the advantages that this could bring in the health sector.

In that field, in fact, distributed registers promise a wide range of applications and functions. Specifically, 'blockchain helps healthcare researchers uncover genetic code by facilitating the secure transfer of patient medical records, managing the drug supply chain, and facilitating the safe transfer of patient medical records'.[18]

Prima facie, a verifiable solution concerns the difficulty of healthcare institutions in sharing information, communicating data, examinations and opinions on the same case or person, providing effective tracking of patient information, and hopefully reducing cases of clinic liability.[19]

The benefit lies in the fact that the various "nodes" could enter all the health information of the individual patient in a system of "blocks" and that, once entered, they could no longer be modified and would only be readable with the required authorisations.[20]

---

[16] Some scholars, in this regard, refer to the emergence of a true virtual identity; personal identity, in the current context, also leads to a new dimension, namely that of information technology, in which personal identity is necessary for the execution of a series of actions, mostly of a patrimonial nature – e.g. the use of credit cards on the web, the various commercial transactions, and even social networks. On this point, S Rodotà, 'Quattro paradigmi per l'identità', in *Vivere la democrazia* (Laterza 2018) 20 ff; G Alpa, 'L'identità digitale e la tutela della persona. Spunti di riflessione' (2017) CONTR. IMPR., 725; G Resta, 'Identità personale e identità digitale' (2007) DIR. INFOR.

[17] P. De Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies (2016) 7 J. PEER. PROD., 1. The author emphasises that despite the obvious advantages they offer in terms of data sovereignty, decentralised architectures also have features that, if not taken into due consideration, could ultimately compromise users' privacy. Indeed, '[w]hile they are capable of preserving the confidentiality of data, decentralized architectures cannot easily protect themselves against the analysis of metadata'. *Ibid.*

[18] A Haleem and others, 'Blockchain technology applications in healthcare: An overview' (2021) INT'L J. INTELLIGENT NET., 132-133.

[19] MS Gross, RC Miller Jr., 'Ethical Implementation of the Learning Healthcare System with Blockchain Technology', in *Blockchain in Healthcare Today* (Berman 2019). For a general overview of liability in healthcare see P Stanzione, V Zambrano, *Attività sanitaria e responsabilità civile* (Giuffrè 1998); M Bassini and others, 'Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?', in F Pizzetti (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, (Giappichelli 2018) 333 ff.

[20] Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (n 1) 219. This represents a purpose from which treating physicians and healthcare facilities can equally benefit to reduce their possible liability, especially where recognised healthcare guidelines have been

It is possible to state how the healthcare system is required to 'to do more with less, find new ways to treat patients more efficiently, and deliver care in alternate settings that help keep patients out of the hospital'.[21]

It would be desirable, in this regard, to improve collaboration between providers through well-organised data sharing systems, to increase the capacity of healthcare facilities and, at the same time, of operators to circulate information, making it more accessible to the majority of those involved with consequent advantages in terms of speed and, above all, economics.[22]

Compared to traditional healthcare systems, in fact, the application of blockchain in this sector has the connotations of preventability, immediacy and interconnection of information.[23]

---

followed, as provided for by Law No. 24/2017 (the so-called Gelli-White Law). The Gelli-Bianco law, adopting the so-called "double track" system, recomposed the interpretation of Article 1228, bringing healthcare workers back into the group of the debtor's auxiliaries who, unlike the latter, who are contractually and objectively liable for their wilful and negligent acts, are liable for their non-contractual and negligent acts. The liability of the healthcare facility that, in the performance of its obligation, makes use of the work of third parties, on the other hand, has been explicitly qualified as "contractual" by the recent reform law, which precisely recalls Articles 1218 and 1228 of the Italian Civil Code (Art. 7, paragraph 1 of the Law). See A Procida Mirabelli di Lauro, 'Inadempimento e causalità "materiale": perseverare diabolicum' (2020) 1 DANNO & RESP., 76. On liability of structures, see amplius G D'Amico, 'Il rischio della "causa ignota" nella responsabilità contrattuale in materia sanitaria' (2018) DANNO RESP., 357 ff; R Pardolesi, R Simone, 'Tra discese ardite e risalite: causalità e consenso in campo medico' (2018) 1 FORO IT., 3582 ff; R Pardolesi, R Simone, 'Nesso di causa e responsabilità della struttura sanitaria: indietro tutta!' (2018) 1 DANNO RESP., 10 ff; A Procida Mirabelli di Lauro, M Feola, 'La cooperazione mancata: sopravvenuta impossibilità della prestazione e imputabilità dell'inadempimento' (2019) COMPARAZIONE DIR. CIV., 33 ff; Stanzione, Zambrano, *Attività sanitaria e responsabilità civile* (n 19); Toscano, 'Il difetto di organizzazione: una nuova ipotesi di responsabilità? (note to Court of Monza June 7 1995)' (1996) RESP. CIV. PREV., 389 ff; I Rapisarda, 'La privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche' (2023) 1 LEGGI CIV. COMM.,184; C Irti, 'L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano' (2023) 1 PERS. MERC., 32-49; M Magliulo, R Pardolesi, 'Pluralità di nessi di causa e paziente allo sbaraglio' (2019) DANNO RESP., 256 ff; F Piraino, 'Il nesso di causalità materiale nella responsabilità contrattuale e la ripartizione dell'onere della prova' (2019) GIUR. IT., 709 ff; G Comandé, 'La riforma della responsabilità sanitaria al bivio tra conferma, sovversione, confusione e ... no-blame giurisprudenziale' (2016) RIV. IT. MED. LEG. the author emphasises how while the natural reference to "liability of the doctor" implicitly referred to an individual contractual liability for inexact fulfilment of the obligations contractually assumed by the professional, subsequently the attention of jurisprudence began to shift towards the extra-contractual liability of the professional whose relationship with the patient appeared difficult to qualify in strictly contractual terms. By the same author, G Comandé, 'Dalla responsabilità sanitaria al no-blame regionale tra conciliazione e risarcimento' (2010) DANNO & RESP., 977-988; G Comandé, 'Le «regioni» della responsabilità sanitaria e il governo del risarcimento', in *"Liber Amicorum" per Francesco D. Busnelli. Il diritto civile tra principi e regole* (Giuffrè 2008) 529-544. See also, FD Busnelli, 'Il fattore "potenziamento": salute, medicina e deontologia al vaglio delle nuove tecnologie' (2017) RESP. MED., 315 ff; A Borroni, 'Gli obblighi a carico del personale e dei liberi professionisti che operano nella struttura, in F Gelli and others, *La nuova responsabilità sanitaria e la sua assicurazione dopo la legge Gelli-Bianco* (Giuffrè 2017) 67-74.

[21] Borroni, 'Blockchain: Uses and Potential Value' (n 7) 41.

[22] A Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (2020) 8 INT. J. INNOV. RES. SCI. ENG. TECHNOL., 159-160.

[23] Through the network, using portable mobile devices, medical personnel can constantly perceive, process, and analyse major medical events (facilitating their preventability and predictability). Likewise, practitioners can grasp the news of each patient's case at any time and quickly develop a diagnosis and treatment plan (thus ensuring immediacy). On this point, Y Li and others, 'Literature Review on the Applications of Machine Learning and Blockchain Technology in Smart Healthcare Industry: A Bibliometric Analysis' (2021) J. HEALTCARE ENG.

Moreover, practitioners can access the medical system anywhere to request images and diagnoses of a patient that are, therefore, "readable" in any hospital through the medical network (in other words, an integral interconnection).[24]

It is worth noting that patient data is held by many different companies[25] and with the advent of the Internet of Things, the quality and quantity of information collected, stored, and provided will constantly increase. [26] Following in this vein, blockchain could lend its support to the aim of protecting users from privacy issues, 'providing also the way to have a unified and more efficient register for the costumers'.[27]

From a practical point of view, such a technological advance would make it possible to register two categories of data: (i) "on-chain" stored directly on the blockchain; (ii) and "off-chain" catalogued in the register through connections 'that act as a pointer to information stored in distinct, traditional databases'.[28]

The storage of medical information directly on the distributed ledger ensures that it is adequately protected by its own structure and is immediately visible to all those with specific authorisation to access the chain.[29]

Given these premises, the positive effects of such a system are innumerable. Consider the case in which a healthcare facility decides to use the blockchain; when an operator visits a patient, he creates an electronic medical record and thus sets up a new block in the chain. Every time the patient carries out examinations or routine checks, his or her file is updated, by means of a new block – which contains both the last report produced and the previous documents[30] – which, in turn, is transmitted to all the nodes.[31]

In this perspective, therefore, the mechanism of consent of the various nodes (via computer) of the chain just described represents a guarantee of transparency, through a safer and more efficient management of patients, medical records and the health data associated with them, as part of a sharable and immutable database that can be freely consulted by medical personnel -

---

[24] *Ibid*. Through the network, using portable mobile devices, medical personnel can constantly perceive, process, and analyse major medical events (facilitating their preventability and predictability). Likewise, practitioners can grasp information of each patient's case at any time and quickly develop a diagnosis and treatment plan (thus ensuring immediacy). Moreover, the medical staff can access the medical system anywhere to request images and diagnoses of a patient that are, therefore, available in any hospital through the medical network (in other words, an integral interconnection).

[25] D Nancy Kirupanithi, A Antonidoss, 'Analyzing the Cost Efficiency Using Attribute Based Encryption on Medical Blockchain Platform' (2020) 11 INT. J. ELECTR. ENG. TECHNOL., 396.

[26] On the role of IoT in healthcare system, N Neranjan Thilakarathne, 'The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study' (2020) 10 INT. J. ENG. MANAG. TECHNOL.

[27] MN Weldon, R Epstein, 'Beyond Bitcoin: Leveraging Blockchain to Benefit Business and Society' (2019) TRANSACTIONS, 863.

[28] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 162.

[29] R Krawiec and others, *Blockchain: Opportunities for Health Care*, (Deloitte 2016).

[30] Neranjan Thilakarathne, 'The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study' (n 26) 147-148.

[31] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 161.

clearly where all the characteristics of the case allow for respect of patient privacy.[32]

Thanks to the immutability of blockchain, as already mentioned, tampering would not be allowed (*rectius*, it would in fact be extremely unfeasible).[33] Unlike traditional databases, in fact, which rely on a centralised server, the use of a distributed system would allow the exchange of information among peers and with higher levels of security.[34]

In addition, a further advantage of medical records based on such a technological system is the possibility of improving interoperability between clinics, hospitals, and other healthcare providers.[35]

The information recorded on the public ledger could be widely accessible through private key systems, allowing patients to exchange their data much more easily with healthcare organisations.[36]

In this vein, technological differences in storage systems often make it difficult to share documents between organisations. Blockchains, conversely, would solve this problem by allowing authorised parties to access a unified database of medical records or even pharmaceutical distribution records.[37]

This would bring other "collateral" advantages affecting: (i) more effective management of the supply chain, (ii) protection from insurance frauds, (iii) clinical trials.[38]

Therefore, the advantage of having at disposal, in any health facility, the entire medical history of a citizen who, at that moment, needs treatment or assistance, re-proposes the need to build and constantly update a huge database whose information must also be treated in respect of privacy, regulated by the General Data Protection Regulation (GDPR) – which will be

---

[32] Borroni, 'Blockchain: Uses and Potential Value' (n 7) 41-42. The blockchain, moreover, should also facilitate the adoption of an Electronic Health Record (EER) since, as of today, for the same patient polyclinics, doctor's offices, hospital companies, individual doctors – each with their own management software – create several files that are often disconnected and the data are, therefore, often incomplete, and difficult to update. Although the analysis of the blockchain-privacy pair will be dealt with extensively in the last chapter, as far as privacy in healthcare is concerned, see, *ex multis*, JL Fernández-Alemán and others, 'Security and privacy in electronic health records: A systematic literature review' (2013) J. BIOMED. INFORM., 541–562.

[33] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 159. In this context, it is very important to ensure the integrity and validity of patient records. Furthermore, the use of algorithms to encrypt the data stored on the blockchain ensures that it can only be decrypted by users with legitimate data access permissions, thus improving data security and privacy. Furthermore, since the identities of clients in a blockchain are pseudonymised using cryptographic keys, patient health information can be shared between healthcare stakeholders without exposing patients' identities. See, on this point, also C Agbo and others, 'Blockchain Technology in Healthcare: A Systematic Review' (2019) HEALTHCARE, 56.

[34] Neranjan Thilakarathne, 'The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study' (n 26) 148.

[35] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 161-162.

[36] *Ibid*.

[37] Agbo and others, 'Blockchain Technology in Healthcare: A Systematic Review' (n 33) 56-57.

[38] A Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 162.

discussed in detail in the last paragraph.

Regarding the handling of information in compliance with the GDPR, briefly, the flexibility in reading the blockchain will undoubtedly make it possible to provide for authorisations, manageable by the patient, in cases where consultation does not take place directly by healthcare facilities – as, for example, in the case of the pharmacy for checking the drugs to be purchased.[39]

It is desirable, therefore, to use "free" – permissioned – blockchains, to avoid that sensitive patient data can be freely consulted by persons who do not belong to the circle of insiders and processed unlawfully.[40]

In this way, GDPR compliance could be achieved where the blockchain is private and legitimised, *i.e.*, where all nodes in the network are known to each other and have the appropriate authorisation to view and add further blocks.[41]

3. Different types of blockchain.

What has been said so far shows that, depending on the objective to be pursued, various technological models may be applicable.

DLTs, in fact, are different from one another and, therefore, recourse to the term blockchain may be generic and misleading, since it is necessary to distinguish, as far as health issues are concerned, at least two main types: those that are permissionless and those that are permissioned[42] – there are, then, others, including hybrid or consortium ones; however, for the purpose of this discussion it will be sufficient to analyse only the first two types.

In particular, whether the aim is to increase the tools of research without any limits or conditions, the use of an open system (permissionless) would undoubtedly be preferable, given the intrinsic advantage of decentralisation and the objective of guaranteeing anyone the possibility of viewing the

[39] Fernández-Alemán and others, 'Security and privacy in electronic health records: A systematic literature review' (n 32) 541-562.

[40] R El Ghazzar, K Stendal, 'Blockchain in Health Care: Hope or Hype?' (2020) J. MED. INTERNET RES., 31-33. In this regard, '[a] proposed workaround is to store the patient data off-chain and have the pseudonym codes stored on-chain'. *Ibid.* See also, Agbo and others, 'Blockchain Technology in Healthcare: A Systematic Review' (n 33) 56; AA Vazirani and others, 'Implementing Blockchains for Efficient Health Care: Systematic Review' (2019) J. MED. INTERNET RES. However, 'this implies that the pseudonym code and any transaction records on the patient data that are stored on-chain would still be existent even after deleting the patient data that were stored off-chain. To reverse the immutability of blockchain, a proof-of-concept prototype for a "forgetting blockchain" was proposed to delete old data from private permissioned blockchains; however, the prototype still has limitations to address'. *Ibid.*

[41] Deborah and others, 'Blockchain: A Possible Alternative to Achieving Health Information Exchange (HIE)' (n 21) 163-164. The distributed register makes it difficult for data subjects, such as patients or providers, to exercise their rights related to the behaviour of a data controller because there is no single data controller, such as an organisation, that acts as the "keeper" of the data, but rather network nodes that each contain a copy of the data. In the EU Data Protection Regulation, rights related to the behaviour of a data controller include the right to access one's personal data, to rectify it, to be informed about its processing, to object to its processing and to have it erased. See, on this point, also Vazirani and others, 'Implementing Blockchains for Efficient Health Care: Systematic Review' (n 40).

[42] Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (n 1) 221.

information contained in the registry and contributing to its management and updating (the basis of the Proof-of-Work scheme on which most blockchains are based).[43]

Conversely, the closed (permissioned) model should be used if the goal is to guarantee the interest of the individual patient, the individual. Permissioned systems, in this sense, can be regarded in the same way as private networks, in which the availability of data depends on the agreement – or rather, consent – of several predefined servers. From an operational point of view, they require an organisation and governance structure with a specific concession to view the register and, usually, basic instructions to access it.[44] In this sense, the approval system is no longer entrusted to the totality of participants but, indeed, to a limited group of nodes, or a single node, with recognised authority (the so-called Proof-of-Authority scheme).[45]

At the end of the day, the technical avenues within the blockchain are different and can be used to facilitate health protection, privacy, research, and healthcare organisation. In such a scenario, it is up to the technicians to study the most effective one to pursue the set goals, but, specifically, it is up to the healthcare organisation to embrace the novelty of data collection.[46]

What emerges, however, from the studies that have been carried out is the

---

[43] M Liu and others, 'How Will Blockchain Technology Impact Auditing and Accounting? Permissionless vs. Permissioned Blockchain' (2019) 13 CURR. ISS. AUD., 4 ff.

[44] DA Zetzsche and others, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) U. ILL. L. REV., 1372.

[45] In this context, '[w]hen new records are added, the ledger's integrity is checked through a limited consensus process carried out by trusted actors'. M Fink, 'Blockchain: Regulating the Unknown', (2017) 19 GERMAN L. J., 670.

[46] On this point, Borroni, 'Gli obblighi a carico del personale e dei liberi professionisti che operano nella struttura (n 20) 67-74. It is prefigurable, *ictu oculi*, a positive obligation of *facere* on the part of the recipients of the same, burdening them with the duty to take part in the clinical risk prevention activities conducted in the facilities in which they serve. In particular, healthcare professionals are required to observe, in the performance of their services, a particularly qualified diligence, appropriate to the nature of the activity exercised (Article 1176, paragraph 2, of the Civil Code) and declined in terms of "expertise", in the sense of compliance with an "ideal" model of conduct that derives from the application of the knowledge and rules of technical-scientific experience proper to the *ars medica*, according to a variable standard in relation to the specific professional category. This perspective represents a significant step forward in the "balancing of burdens" on those involved in the exercise of the health profession and allows the Italian system to align itself with the evolved systems of risk prevention and management typical of foreign experiences, first and foremost that of the United States, following an imitative approach already adopted in other areas of law. As highlighted by G Alpa, 'La responsabilità medica' (1999) 21 *Rivista Italiana di Medicina Legale e del Diritto in campo sanitario*, 15 ff, a new paradigm has been created whereby the "patient monad" and the "healthcare monad" are set in opposition from a civil law perspective, the latter including the healthcare facility and the personnel and means at its disposal. Think of the use of algorithms to improve the collection and processing of personal data relating to the health of individuals, for diagnostic or scientific research purposes. For an analysis on the subject see U Ruffolo, 'L'Intelligenza artificiale in sanità: dispositivi medici, responsabilità e ''potenziamento''' (2021) GIUR. IT., 502 ff; G. Pascuzzi, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche* (Zanichelli 2020); P Guarda, '"Ok Google, am I sick?": Artificial Intelligence, E-Health, and Data Protection Regulation' (2019) 1 BIODIRITTO, 359 ff; G Finocchiaro, 'Intelligenza artificiale e diritto. Intelligenza artificiale e protezione dei dati personali' (2019) GIUR. IT., 1657 ff; G Pascuzzi and others, *Comparative Issues in the Governance of Research Biobanks. Property, Privacy, Intellectual Property, and the Role of Technology* (Springer 2013); U Izzo, P Guarda, 'Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato' (2010) *Trento Law and Technology Research Group Research Papers*.

delays in the digitisation of health data of the patients, more than anything else because of justified fears related to the management of sensitive data, the leakage of which can be particularly detrimental to the rights of the citizens concerned, so that the need to combine both the interest in the circulation of data and the need to use techniques that guarantee privacy rights to the citizens is even more pressing, and in this perspective, precisely, blockchain may represent a viable solution.[47]

4. Health protection and data protection.

In the light of the conducted analysis, there are many points of interest involving the protection of personal data.

In the contemporary global scenario, the new dynamics of information collection and processing, the greater invasiveness of control over individuals, both by public and private entities, have led to an ever-increasing demand for protection.[48]

This discussion is of interest in relation to the regulation of the processing of so-called super-sensitive data, such as health data, since there is a need to define a reasonable balance between the right to health, which requires that the provision of services necessary to safeguard the health and physical integrity of the person concerned and of third parties should not be hindered, and an adequate maintenance of the guarantees prescribed to protect privacy.[49]

In the processing of health information, in particular, data protection provisions are normally 'supplemented by administrative laws that govern retention, resulting in different obligations and conservation timescales, deontological rules and sectoral norms. The scenario is characterized by the coexistence of normative sources and different actors, given a strong need for self-regulation'. [50] However, considering the sensitivity of the data to be

[47] Catelani, 'Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain' (n 1) 222-223.

[48] On this point, G Resta, 'Le persone e la famiglia. Le persone fisiche e i diritti della personalità', in G Alpa, G Resta, *Trattato di diritto civile*, directed by R. Sacco (Giappichelli 2019) 145 ff. The author privileges a "value-oriented" interpretation, considered the most appropriate line for dealing with issues concerning the person and personality rights. In this scenario, the globalisation of markets and the evolution of technologies constitute, for the authors, complex challenges to the role of law.

[49] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 183. See, generally, on privacy and blockchain M Seghesio, 'Blockchain and Privacy', in Borroni, 'Blockchain: Uses and Potential Value' (n 7) 138 ff. In particular, in the current globalised panorama, the gravitational centre of gravity of the right to privacy is increasingly identified, rather than in the right to be "left alone", in the possibility of each subject to control the use of the information that concerns him or her and in considering the problems of privacy in the framework of the current organisation of power, of which the information infrastructure now represents one of the fundamental components. S Rodotà, 'Tecnologia e diritti (Zanichelli 1995) 19.

[50] M Arisi, P Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (2020) BIOLAW J., 489. With regards to the italian context, see E Lamarque, 'Privacy e Salute', in G Losano (ed.), *La legge italiana sulla privacy - Un bilancio dei primi cinque anni*, (Cacucci 2001) 338-339. For

processed, Privacy and Data Protection are certainly key issues for the healthcare applications, eHealth requiring specific attention as it introduces new use-cases and vulnerabilities.[51]

The first aspect is related to data accessibility. In this perspective, it is reasonable to associate the increasing transparency of information with a decreasing respect for the right to privacy.[52]

In fact, the data contained within the blockchain registry are physiologically public; an aspect, this, that would seem to collide – at least *prima facie* – with the data processing rules provided for by European Regulation no. 679/2016 (GDPR).[53]

Transposing this assertion to the blockchain systems used, it is crucial to identify specific arrangements to ensure that access and processing activities are restricted and authorised only in favour of certain persons and in such a way as to enable the integrity of the entire database, also by means of appropriate security measures.[54]

From a different point of view, however, critical elements could be found in relation to the principle of information minimisation, which presupposes the definition of limited retention times. In fact, the data in the blockchain are stored indefinitely fulfilling the guarantees of certainty and verifiability over time, and once they become part of the chain, they are recorded permanently and unalterably within it.[55]

---

instance, Guidelines and Opinions by the Italian Data Protection Authority are fundamental to the interpretation of the legislative content; on this point see GM Riccio, 'Privacy e Dati sanitari', in F Cardarelli and others, *Il Codice dei dati personali - Temi e problemi* (Giuffrè 2004); G Finocchiaro, 'Privacy e protezione dei Dati personali – Strumenti Operativi' (Zanichelli 2012) 295-317.

[51] *Ibid*.

[52] Be permitted a reference to F Zambardino, 'La blockchain nel mercato del lavoro italiano con particolare enfasi sulla questione privacy e il rapporto con il General Data Protection Regulation' (2022) 3 TSL, 23-38.

[53] On the relationship between GDPR and data protection G Alpa, 'La "proprietà" dei dati personali, in Persona e mercato dei dati. Riflessioni sul GDPR', in N Zorzi Galgano (ed.) (Giuffrè 2019) 17 ff; G Finocchiaro, 'Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali' (Zanichelli 2017) 101 ff; L Bolognini and others, *Il Regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali* (Giuffrè 2016) 277 ff. Before the entry into force of the GDPR with particular reference to the processing of health data, 'the former Privacy Code (Legislative Decree 196/2003) provided that the same could be processed only with the consent of the person concerned and after authorization from the Guarantor (art. 26, paragraph 1). In other words, the consent of the interested party was given a central role as a legitimate prerequisite and condition of lawfulness of the processing of personal data. Therefore, the rule was that the personal data could be processed only with the consent of the person concerned and exceptions were provided for (and justified) only by the extraordinary nature of certain situations'. F Rosa, 'The use of it tools and artificial intelligence in the health sector: the patient as a vulnerable subject' (2020) 2 EJPLT, 225-226.

[54] AM Gambino, C Bomprezzi, 'Blockchain e protezione dei dati personali' (2019) DIR. INFOR., 620 ff. See for a general overview Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 477-496; P Guarda, L Petrucci, 'Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati' (2020) BIOLAW J., 425-446.

[55] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 184. In This would run the risk of, on the one hand, undermining the main rights of data subjects under Articles 15 to 22 of the European Regulation, such as the right to obtain the updating, rectification or integration of personal data concerning them, and, on the other hand, of rendering ineffective the requirements of deletion, anonymisation or destruction of data in the event of cessation of processing.

The primary need that remains is to find the right balance between the use of DLTs – in all spheres, but specifically the one under analysis – and the protection of personal data, so that the principles of "data protection by design and by default" can concretely become the necessary starting point for the development of *secundum legem* technological solutions.[56]

It is possible, therefore, to state that blockchain can be compatible with the protection of health data; in light of the technical-operational features described, it would seem to be feared that it might even be possible to fulfil certain obligations to protect the information contained in the registry, in the event that one opts for so-called "permissioned" systems – *i.e.* private ones, as discussed in the preceding paragraph.[57]

Moreover, the use of this technology is fully in line with the recent positions of the European Parliament, summarised in a Resolution of 3 October 2018.[58]

Firstly, the importance and applicative instrumentality of blockchain and, more generally, of any distributed system is grasped; secondly, among the application profiles examined, particular attention is paid to the healthcare sector. The latter, according to the Resolution, could benefit greatly from the use of DLT, in terms of greater control by citizens over their own data, as the maximum expression of their deterministic power, being able to choose which information to share; such a dialogic contribution would translate into increasing levels of transparency, while considering the need to safeguard the confidentiality of the data processed.[59]

At the same time, it is also possible to identify several critical profiles that collide with the protection of privacy. Starting from the assumption that, in the field of DLTs, data are considered pseudonymous and not anonymous, they require the adoption of the measures established by the GDPR.[60]

---

[56] In such a scenario, Article 25 of the GDPR on data protection by design requires the data controller to implement appropriate technical and organisational measures aimed at effectively implementing data protection principles, such as minimisation, and at incorporating the necessary safeguards into the processing to meet the requirements of this Regulation and to protect the rights of data subjects. Gambino, Bomprezzi, 'Blockchain e protezione dei dati personali'(N 54) 624-625. In particular, the GDPR entrusts the data controller with the choice of the most suitable solutions for achieving the objective of risk management, arising from the processing of personal data, and stipulates that he or she will be held accountable if problems arise. Be permitted a reference to F Zambardino, 'La blockchain e la protezione dei dati personali: una tecnologia privacy compliant by design?' (2022) 2 EJPLT, 136-152. See also R Carleo, Il principio di accountability nel GDPR: dalla regola alla auto-regolazione' (2021) NUOVO DIR. CIV., 366 ff; G Comandè, 'Responsabilità e accountability nell'era dell'Intelligenza Artificiale', in F Di Ciommo, O Troiano, *Giurisprudenza e Autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi* (La Tribuna 2018) 1010 ff; M. Trapani, 'GDPR e Intelligenza Artificiale: i primi passi tra governance, privacy, trasparenza e accountability', in A Mantelero, D Poletti (eds.), *Regolare la tecnologia: il Regolamento UE 2016/679 e la protezione dei dati personali* (Pisa University Press 2018).

[57] Be permitted reference to Zambardino, 'La blockchain e la protezione dei dati personali: una tecnologia privacy compliant by design? (N 56) 136-152.

[58] European Parliament resolution of 3 October 2018 on distributed ledger and blockchain technologies: building trust through disintermediation (2017/2772(RSP)).

[59] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 186.

[60] In particular, the aspect of pseudonymisation of personal data (*i.e.,* 'data can no longer be attributed to a specific individual without the use of additional information' Art. 4, no. 5, GDPR) is specifically regulated by

One of these is, definitely, the governance issue. In order to 'implement data protection roles in a blockchain healthcare project may be challenging because definition of data protection roles in the sector can be complex per se and has been debated through timeì.[61] For instance, with reference to the management of health records, exchange of data takes place in diverse environments, presenting different structures according to more than one organizational practice; on this matter, digitalization is ultimately contributing to create a new scenario:[62] the possibility 'to build a blockchain that can mirror the logic of this complex data exchange represents a great opportunity'.[63]

However, the most challenging critical element is that relating to the difficulties inherent in the proper exercise of the rights of the protected subject, placing particular emphasis on the right to be forgotten, which is, moreover, the subject of recent and further hermeneutic discussions.[64]

The last valuable aspect of the Resolution can be found in the identification of the competent Authority to provide a more precise framework on the point: indeed, from the analysis of Article 32, the Parliament invites the European Commission and the European Data Protection Supervisor to provide further guidance on the point.

A dynamic landscape is therefore foreshadowed, disseminated by soft law activities and collaborative relations between the network of competent independent authorities.[65]

---

the GDPR and is subject to the condition that the additional information is "stored separately" and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.

[61] Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 494. See also, more generally, P Guarda, *Fascicolo Sanitario elettronico e protezione dei dati personali* (Università degli Studi di Trento 2011) 106.

[62] P Guarda, 'I Dati sanitari', in V Cuffaro and others, *I dati personali nel diritto europeo* (Giuffrè 2019) 609-617.

[63] Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 494.

[64] The relationship between the right to be forgotten and the right to report news was the subject of a question referred to the United Sections of the Supreme Court of Cassation, which ruled in Judgment No. 19681 of 22 July 2019. On that occasion, the United Sections reiterated the constitutional relevance of both the right to report news and the right to oblivion, specifying that when a piece of news, previously disseminated in the legitimate exercise of the right to report news, is disseminated again, the right of the person concerned to maintain anonymity over his or her personal identity prevails. For more details see the recent contribution by F Balducci Romano, 'La Corte di giustizia 'resetta' il diritto all'oblio' (2020) FEDERALISMI. For an examination of the legal concept of forgetting, see A Palmieri, R Pardolesi, 'Polarità estreme: oblio e archivi digitali' (2020) 1 FORO IT., 1570 (comment to Cass., sez. I, 27 marzo 2020, n. 7559); R Pardolesi, 'Oblio e anonimato storiografico: «usque tandem...»?' (2019) 1 FORO IT., 3082 (comment to Cass., sez. un., 22 luglio 2019, n. 19681); S Martinelli, 'Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in Internet e le problematiche poste dalla de-indicizzazione' (2017) DIR. INFOR.; R Pardolesi, 'Diritto all'oblio, cronaca in libertà vigilata e memoria storica a rischio di soppressione' (2016) 1 FORO IT., 2734 (comment to Cass., sez. I, 24 giugno 2016, n. 13161).

[65] Farina, 'Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?' (n 4) 186-187.

5. Blockchain and telemedicine.

One of the most promising uses of blockchain in the healthcare sector is potentially that related to telemedicine, which makes use of innovative and in some ways still developing technologies to provide care services in contexts of physical distance between the actors involved.[66]

As is well known, telemedicine makes use of Information and Communication Technologies (ICT) to facilitate the secure sharing of medical data in any digital form, useful for prevention, diagnosis, treatment, and examination activities.[67]

Although they can be compared to traditional healthcare services and although they must respect all their rights and obligations, telemedicine services do not totally replace them, but their integration guarantees statistically superior results.[68]

Specifically, the adoption of telemedicine systems in the healthcare sector brings about new dynamics of cooperation between patients and operators, contributing to a concomitant improvement in the services offered. Firstly, in terms of quality of care, since patients' parameters can be constantly monitored remotely; secondly, greater coverage, understood as agility in providing healthcare to individuals living in areas that are difficult to access or distant from hospital facilities; thirdly, greater effectiveness and efficiency, through constant interaction between the various actors involved; and finally, also in economic terms, the optimisation of resources brings as a first consequence a rationalisation of social-health processes, allowing a significant reduction in costs.[69]

Amongst the various positive elements that have been outlined in the previous paragraphs, there also remains the risk of a possible data breach and, consequently, fears in terms of patient privacy. Indeed, centralised systems are vulnerable to external attacks by hackers and malicious users; this represents an element of mistrust towards remote services that often leads to a preference for traditional methods.[70]

---

[66] For a general discussion on the subject, see, NM Hjelm, 'Benefits and drawbacks of telemedicine' (2005) J. TELEMED. TELECARE, 60-70.

[67] Among the first in Italian doctrine U Izzo, 'Medicina e diritto nell'era digitale: i problemi giuridici della cibermedicina' (2000) DANNO RESP., 807 ff. It is clear that telemedicine involves at the same time different disciplines: telecommunications, information technology, and medicine. Telemedicine is seen as a rib of the Anglo-Saxon concept of "telehealth" and "telecare", which lead to a systematic refurbishing of the health system, from the organization and management to the training and education of patients and medical operators. Blockchain technology ensures then a secure interchange of data, imageries, and papers among the patients and medical staff, prevention, analysis, cure, and monitoring can be done without physical presence of the doctor or at the healthcare facilities.

[68] K Griggs and others, 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring' (2018) J. MED. SYST'S, 42 ff.

[69] E Funk '*Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education* (2019) 93 J. ASS. AM. MED. COLL., 93 ff.

[70] Griggs and others, 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring' (n 68) 42 ss.

The effectiveness of virtual care and health monitoring depends on the integrity of Electronic Health Records (EHRs), which include a patient's medical history, diagnosis, medication, and treatment plans.[71] EHRs contain highly sensitive and private information, which needs to be shared securely between facilities – hospitals, pharmacies, and health authorities – to keep medical data up to date.[72]

The introduction of blockchain in this context would foreshadow a strengthening of trust, given the lack of intermediaries inherent in this technology. By means of this system, the management of consent is secured and protected by several "peers" belonging to different and "distributed" participating organisations.[73]

A further issue is the difficulty for healthcare organisations to manage the quantity of patient records due to limited interoperability.[74] To overcome this impasse, blockchain provides a single, consistent view of electronic patient records for all participating stakeholders. The visibility and transparency of information allows participating organisations to trace a patient's medical history to propose appropriate treatment.[75]

Virtual healthcare systems based on online advice, in addition, require the practitioner to enter patient's data into the registry sharing the prescription of drugs with pharmacies. Through hash functions, the blockchain can help eliminate potential prescription errors.[76] Registered pharmacists can access prescriptions to verify, prepare and send drugs to patients. And, in this sense, transparency and traceability can also allow patients and doctors to verify the actual "originality" of the drug by analysing its provenance.[77]

---

[71] In Italy, Article 12 of the decree law no. 179/2012 regulates the electronic health record and surveillance systems in the health sector, in which the concept of the health record is defined, but more than anything else the underlying objectives are identified, including the reference to guaranteeing health, facilitating scientific research and purely organisational profiles, such as health planning, verification of the quality of care and evaluation of health care. Guarda, *Fascicolo Sanitario elettronico e protezione dei dati personali* (n 61) 106 ff.

[72] The legal definition of the EHRs in the regulatory context of personal data protection cannot but reflect a vision of care that the National Health System as a whole (a system in which public and private subjects take their place with differentiated, but increasingly integrated roles and responsibilities) intends to pursue, in the awareness that information assumes, today more than ever, a key role in any process traceable to the ideal objective of protecting the health of the citizen/patient/interested party. Pascuzzi, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche* (n 46) 86.

[73] P Genestier and others, 'Blockchain for consent management in the ehealth environment: a nugget for privacy and security challenges' (2017) J. INT. SOC. TELEMED. EHEALTH., 5 ff.

[74] Arisi, Guarda, 'Blockchain and eHealth: seeking compliance with the General Data Protection Regulation' (n 50) 489. The authors state that '[t]he need for interoperability, selective access and security and integrity of data are an essential feature of this sector and this is why several blockchain-based projects can be found, but the reference is especially to the opportunities related to private and permissioned blockchains, which ensure confidentiality of the data'.

[75] RW Ahmad and others, 'The role of blockchain technology in telehealth and telemedicine' (2021) INT. J. MED. INFORM., 6.

[76] Y El-Miedany, 'Telehealth and telemedicine: how the digital era is changing standard health care' (2017) SMART HOMECARE TECHNOL. TELEHEALTH., 45-46.

[77] Ahmad and others, 'The role of blockchain technology in telehealth and telemedicine' (n 75) 7.

Finally, a side advantage can also be found regarding insurance. For example, in the case of insurance fraud (think of the submission of an incorrect claim for treatment costs to an insurance company), the administrative costs of establishing the veracity of the information provided are high. Blockchain technology can help both insurers, in terms of minimising insurance fraud (by authorising them to access a patient's medical record), and policyholders (*i.e.,* patients) who can be incentivised to provide consent to use their medical data for insurance purposes. [78] The growing need to collect information on customers for the purpose of tailoring personalised products on them, calibrated to risks monitored either through digital devices or diagnostic tools, is, in a way, contextualised.

However, it should be emphasised that telemedicine systems, to function properly, require close coordination between the actors involved in healthcare processes, to maintain a consistent and up-to-date patient history and reduce diagnostic errors.[79]

Conclusive remarks.

The application of blockchain in healthcare has still encountered many difficulties, especially regarding privacy, data management and control, given the resistance of this sector to embrace new technologies or change its organisational patterns.

This is true if one considers the internal structure of DLTs, based on the building block. The medical history is permanently compiled and available to all practitioners wherever they are, supporting the necessary procedures to efficiently activate mechanisms such as telemedicine and remote assistance.

As far as increasing security is concerned, it is worth remembering that whenever data is entered by a node, it cannot be damaged, altered or deleted and, at the same time, the patient can control who has entered a piece of data and who has read it, with a mechanism of maximum transparency.

From this point of view, this can be advantageous in reducing the liability of doctors and healthcare facilities, especially if this is linked to specific guidelines to be followed.[80]

---

[78] *Ibid.*

[79] Griggs and others, 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring' (n 68) 42 ff. On the matter see also F Cerea, 'Intelligenza artificiale a servizio dei pazienti per il contrasto a CoViD-19' (2020) NUOVA GIUR. CIV. COMM., 45 ff.

[80] On the matter, PG Monateri, 'La responsabilità civile', in *Trattato di diritto civile*, directed by R. Sacco (Giappichelli 1998) 753 ff. The author states that just as medical liability constituted a subsystem of the latter within civil liability, so too within contractual liability it nevertheless continues to present profiles of marked peculiarity. However, since the liability approach necessarily implies that the damage has occurred, the perspective to be taken, especially in the health sector, is that of security, including cyber security, which is the way to provide manufacturers of digital health solutions, as well as health professionals and users of these solutions, with rules, protocols and tools to prevent and reduce the risks that these solutions may present. G Capilli, 'Innovazione tecnologica e responsabilità: un breve sguardo alla "sanità mobile"

The implications of using blockchain are manifold and vary depending on the perspective of the users (be they patients, doctors, or the facilities themselves); at present, however, understanding of the potential of the technology (and blockchain in particular) is still "opaque". Involvement in medical insurance, in emergency cases, in product testing, in monitoring through statistical tools and mathematical or geometric graphs, are just some of the areas where the investigation is at least promising.[81]

(mHealth)' (2023) 1 EJPLT, 69-70. Legal scholars, in analyzing liability arising from the use of technology – *latu sensu* – in the medical field, have made reference to the standard provided by the Article 2050 of the Italian Civil Code related the assumption of liability for individuals who engage in activities that are particularly dangerous and potentially offensive to third parties. The activity taken into consideration is that which, by its nature, or the nature of the means employed, is defined as "dangerous". See P Perlingieri, 'Responsabilità civile e robotica medica' (2020) TECN. DIR., 165 ff.

[81] The consequences and the possible effects in the hiring process are manifold if it considered the power of an employer that could have potentially access to a candidate's health information and verify chronic pathologies, some latent physical difficulties, the days and places in which treatments took place and visits, any vaccinations, the number of days of illness and thus drive one's choice with an impact that ranges from contracts in the world of sport to more sedentary jobs. Indirectly, then, this availability of information would also lead to indirect control of the conduct of the doctors and eventual medical malpractice.

Gatt L, Caggiano IA, Gaeta MC, Aulino L, Troisi E, 'The possible relationships between law and ethics applied to AI' (2023) 2 EJPLT, 111 - 120.
DOI: https://doi.org/10.57230/EJPLT232GCG

EJPLT
ISSN 2704-8012



The possible relationships between law and ethics applied to AI*

Le possibili relazioni tra legge ed etica applicate all'IA

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

LIVIA AULINO
Ph.D., Senior Researcher of the Research Centre in European Private Law (ReCEPL)
Suor Orsola Benincasa University of Naples
Post-doc in Private Law, University of Naples Federico II

EMILIANO TROISI
Ph.D., Junior Researcher of the Research Centre in European Private Law (ReCEPL)
Suor Orsola Benincasa University of Naples

Abstract

The paper aims to critically analyse and compare legal rules and ethical principles in order to understand their possible relationships in the regulation of artificial intelligence systems. Indeed, the purpose of the work is to identify the interaction of law with ethics to guarantee an adequate regulation of AI, also in terms of sustainability, defining the measuring methodologies of the impact of AI on individuals under an *ex ante* and *ex post* perspective.

Il lavoro si propone di analizzare e confrontare criticamente le norme giuridiche e i principi etici per comprendere le loro possibili relazioni nella regolamentazione dei sistemi di intelligenza artificiale. Lo scopo del lavoro è infatti quello di individuare l'interazione tra diritto ed etica per garantire un'adeguata regolamentazione dell'IA, anche in termini di sostenibilità, definendo le metodologie di misurazione dell'impatto dell'IA sugli individui in una prospettiva ex ante ed ex post.

The work was presented at the IEEE International Conference 'Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering' (MetroXRAINE), held at National Research Council, Milan, October 25-27, 2023.

© The author(s) 2023, 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: E&L; regulatory perspectives; ethical-legal compliance by design; risk analysis.

Summary: 1. Introduction: Law & ethics. – 2. The regulation of Artificial Intelligence through two types of rule sets: legal and ethical. – 3. Identification and analysis of tools on the impact of AI. – 4. First conclusions on how to measure the impact of AI on individuals.

1. Introduction: Law & ethics.[1]

The starting point of the paper is the relationship between law and ethics, then deepened with regard to the artificial intelligence (AI) domain, where the interaction between law and ethics is of particular relevance.

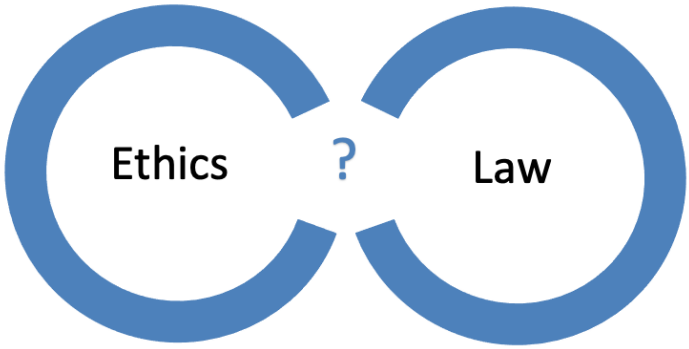


Figure 1: The difficult relationship between law and ethics

Legal positivists are used to study and apply binding law but, sometimes, the issue of identifying the applicable law in some specific field (e.g. artificial intelligence) has highlighted the need to resort to other sources of regulation, such as ethical principles. This need has been a consequence of a lack of *ad hoc* binding legal regulation for many years in a specific domain and the proliferation of ethical principles with the function of guiding individuals, companies, and institutions in the regulation of a specific phenomenon.

The legal system is not incomplete, but it cannot regulate every single phenomenon, being possible to apply the principles of *analogia legis* or *analogia iuris*, or just the extensive interpretation of the existing legislation

[1] 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 Vice-director Prof. Ilaria A. Caggiano. The author of paragraphs 1, 2 and 4 is Maria Cristina Gaeta, Ph.D., Lecturer in Private Law and Scientific Secretary of the Research Centre in European Private Law (ReCEPL), Università degli Studi Suor Orsola Benincasa; the authors of paragraph 3 are Livia Aulino, Ph.D., Senior Researcher of the Research Centre in European Private Law (ReCEPL), Università degli Studi Suor Orsola Benincasa, and Post-doc in Private Law, Università degli Studi di Napoli Federico II, and Emiliano Troisi, Ph.D., Junior Researcher the Research Centre in European Private Law (ReCEPL), Università degli Studi Suor Orsola Benincasa.

(according to art. 12 of the preliminary provisions to the Italian civil code), when an *ad hoc* legislation is missing.

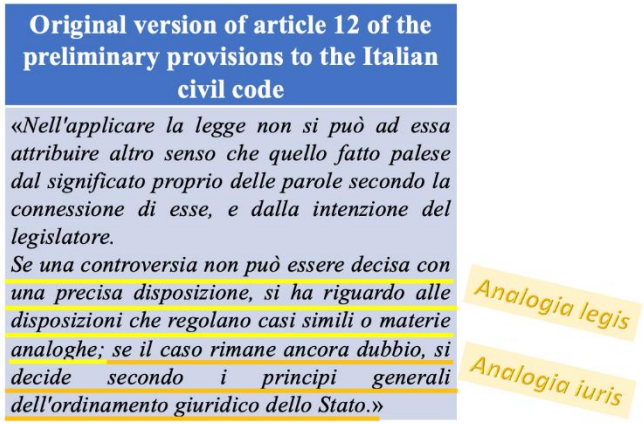


Figure 2: Quotation of the article 12 of the preliminary provisions to the Italian civil code

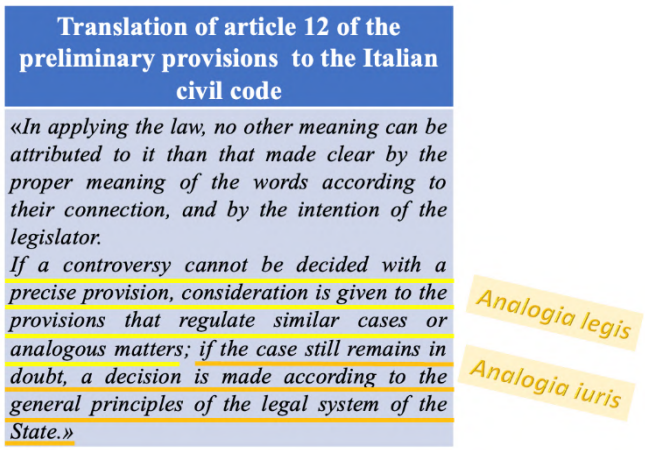


Figure 3: English translation of the quotation of the article 12 of the preliminary provisions to the Italian civil code

In this context of interpretation of the law, it is important to understand the role of ethics.

The academic literature[2] has already underlined that it is not possible to interpret the law according to ethical principles, otherwise, the interpretation of the law would involve discretionary choice arising from the ethical values. For example, on issues such as abortion or medically assisted procreation (MAP), which are widely debated by ethical scholars, the interpretation of the law cannot be based on such values, which could be absolutely against abortion or MAP. On the contrary, the interpretation of the law according to criteria of

[2] G Iudica, 'Etica versus diritto', in LA Bianchi, F Ghezzi, M Notari (eds.), *Diritto, mercato ed etica. Dopo la crisi. Omaggio a Piergaetano Marchetti* (Bocconi University Press, 2010), 157 ff.; P Schlesinger, 'Morale e diritto', in LA Bianchi, F Ghezzi, M Notari (eds.), *Diritto, mercato ed etica. Dopo la crisi. Omaggio a Piergaetano Marchetti* (Bocconi University Press, 2010), 903 ff.; D Plunkett, 'Legal Positivism and the Moral Aim Thesis', in Oxford J. Legal Studies, 2013, 563 ff.; HLA HART, 'Positivism and the Separation of Law and Morals', in [1958] Harv. L. Rev., 593 ff.. V Cariello, *Paradigmi e linguaggi intepretativi* (Giappichelli, 2022), XIX ff.

the first and second paragraphs of art. 12 of the preliminary provisions to the Italian civil code, would ensure an objective application of the law, through the elaboration of a legal norm that does not consider ethical choices. In this case, indeed, abortion or PMA can be allowed, under certain conditions and within certain limits.

At the same time, however, other part of the academic literature[3] considers that ethical principles can be also a criterion for the interpretation of the law, but only if ethical values are in compliance with hard law (*secundum legem*), even if in this scenario the role of ethics would be very much limited, like that of a custom[4] because in this case, ethical values would have the function of strengthening the reason of the law (so-called *ratio legis*), making it explicit in the interpretation/application phase of the law.

Indeed, private law has to be interpreted in the light of art. 12 of the preliminary provisions to the Italian civil code, in particular, systematic and evolutionary interpretation are of great relevance to guarantee the application of the law in line with the evolution of contemporary society, and ethical values can have a role in the interpretation of the law only if they are *secundum legem*. According to authoritative doctrine, the theory of interpretation under art. 12 of the preliminary provisions to the Italian civil code, then, cannot be kept separate from the theory of interpretation in compliance with the constitutional rules, considering that the idea of society and of ethics underlie the Constitution.[5]

Having thus identified the relationship between ethics and law at the stage of interpretation of the law, it is important to consider this relationship when ethical principles are transposed into law[6]. More precisely, this means that ethical values have been positively underpinned by certain legislative choices, being transposed into binding law, and becoming binding rules themselves. Indeed, ethical considerations can ground legal norms, even the most fundamental ones: constitutional rights and international treatises. In this way, social sciences (law and philosophy) influence one another, even though each domain maintains its specificities.[7]

The third possible scenario concerns the integrative role of ethics in cases of lack of specific legislation of a phenomenon. This is that hypothesis in which the law has to be applied to a new legal case according to the principle of *analogia* (*legis* or *iuris*), but in itself is not sufficient for an efficient and effective regulation of the phenomenon. In this circumstance, other rules can supplement the regulation. First and foremost, soft law acts (from guidelines to codes of ethics), which, although not binding, have a strong power to

[3] L Green, 'Positivism and the Inseparability of Law and Moral' [2008] New York Univ. L. Rev., 1040 ff.
[4] A Bertolini, Regulating UncertAInty, Description of the Conference of EURA Jean Monnet Centre of Excellence, 8-9 april 2021.
[5] P Perlingieri, *Il diritto civile nella lergalità costituzionale* (3rd ed., ESI, 2006), pp. 560 ff.
[6] European Parliament Report with Recommendations to the Commission on Civil Law Rules on Robotics, 24.01. 2017, (2015/2103(INL)), letter W of the General principles, p. 6.
[7] A Bertolini, G Aiello , 'Robot companions: A legal and ethical analysis' (2018) 34(3) The Information Society, 130 ff.., see also A Bertolini, 'Governare il potenziamento umano attraverso i principi di dignità e uguaglianza. Appunti per un quadro teorico-dogmatico di riferimento'(2022) 3 Politica del diritto, 435 ff.

orientate citizens and Institutions.[8] To these soft law acts must then be added the technical regulation (i.e. standards), which are also applicable through express referral by law, as well as techno-regulation. By techno-regulation is intended the possibility of using technologies also as instruments of regulation and not only as objects of the regulation (e.g. data protection and security by design and by default).[9]

2. The regulation of Artificial Intelligence through two types of rule sets: legal and ethical.

The latest academic discussion has focused on the potential and risks associated with new technological systems. In this perspective, defining a set of legal rules, that properly regulates these technologies, could be the priority, but this action appears extremely difficult and, therefore, in the last years, only a set of ethical principles contained in many different documents has been published by European and International Institutions, before the publication of the most recent European regulatory proposals on AI (the Proposals of Artificial Intelligence Act - AIA, Artificial Intelligence Liability Directive - AILD, and Product Liability Directive revision - PLD revision)[10].

For this reason, starting from the current state of the art, the paper is based on the legal and ethical challenges arising from the development of new technologies, with particular regard to AI, in order to define how to measure the AI Impact on individuals, elaborating the steps necessary to evaluate its risks, according to preventive and remedial analysis. Only after a proper analysis of the impact of AIs will be possible to provide an effective and efficient regulation according to the level of the risk of the AI system.

The need to analyse the impact of AI is a consequence of the fact that new technologies development has not only entailed benefits for the human being but also multiple risks ranging from a data breach to a cybersecurity breach, as well as a physical injury or psychical manipulation. For this reason, it is necessary to verify AI's impact and consequently intervene by regulating AI to limit the legal and ethical risks for human beings related to the use of technological systems and, instead, to fortify their benefits. This idea is currently foreseen by the Artificial Intelligence Act proposal, which classifies AIs based on the

[8] A Iannotti della ValIE, 'L'età digitale come "età dei diritti": un'utopia ancora possibile?' (2019) 16 Federalismi 10; E Mostacci, *La soft law nel sistema delle fonti: uno studio comparato* (Wolters Kluwer, 2008), 117 ff; A Somma, 'Soft law sed law: diritto morbido e neocorporativismo nella costruzione dell'Europa dei mercati e nella distruzione dell'Europa dei diritti' (2008) 3 Rivista critica del diritto privato, 437 ff..

[9] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018.

[10] Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 21.4.2021, COM(2021) 206 final, and following revisions; Proposal for a Directive of the European Parliament and of the Council, on adapting non-contractual civil liability rules to artificial intelligence (Artificial Intelligence Liability Directive), 28.9.2022, COM(2022) 496 final; Proposal for a Directive of the European Parliament and of the Council on liability for defective products (Revised Product Liability Directive), 28.9.2022, COM(2022) 495 final.

possible risks (high risk, low risk and prohibited), so that different regulation can be envisaged according to the level of risk of the AI system for individuals.

Such a risk-based classification of AI systems, and the consequent different regulation, ensures a fair balance between the need to foresee and prevent the risks associated with the development of AIs, on the one hand, and the non-excessive restriction of the design and production of AIs that have a positive impact, on the other. In fact, the provision of too restrictive legal rules could constitute a limitation for the development of AI (as for instance in the case of some provider/producer objective liability schemes), which, however, may be the best possible solution for preventing risks to individuals. This is why it is necessary to adequately classify the levels of AI to enable providers/producers to act within the regulatory framework of reference for that level of AI involved, guaranteeing their necessary autonomy but within the limits laid down by the regulations for the protection of individuals.

Concerning the AI regulation, the introduction of ethical principles has proceeded that of the legal ones. Ethics does not provide binding legal rules, but has social and moral value and is of particular importance in relation to new technologies for two reasons: (i) firstly because of the impact of AI on human beings; (ii) secondly, because initially (before 2021) the European legislator was not ready to regulate the phenomenon through binding regulation able to really understand new technologies and being able to keep up with its development. During the last years (2021 and 2022), instead, the European Union started to translate these ethical principles into legal rules, that now constitute regulatory proposals but which will become binding rules in the near future. Ethical principles would remain to complement and supplement the law but would largely be transposed into these binding rules. In this way, the ethical principles implemented in European regulations would become binding rules.

More in detail, the International Institutions, the European Union, and its Member States have always been founded on the values of human dignity, equality, solidarity, freedoms, and respect for human rights,[11] and this approach is being applied also regarding robotics and artificial intelligence. The legislators are now called to intervene to guarantee the protection of human beings in relation to new technologies also with binding rules. In fact, AI technologies are not neutral and, in addition to entailing a series of advantages, it also implies serious risks for individuals who have a structural condition of vulnerability in relation to them.[12] Therefore, new technology, especially when equipped with AI, must be properly regulated, to put these new technologies at the service of humans.

In this light, at all levels of regulation, the awareness of the need for a concrete strategy and regulation of AI has matured. In particular, in May 2019, the Council of Europe adopted some recommendations aimed at maximising the potential of AI systems and preventing a negative impact on human

[11] Universal Declaration of Human Rights of the United Nation (UDHR) of 10 December 1948; European Convention on Human Rights (ECHR) of 4 November 1950; Charter of Fundamental Rights of the European Union of 18 December 2000 (FREU); National Constitutional Charters.

[12] L Gatt, IA, Caggiano, 'Consumers and digital environments as a structural vulnerability relationship' (2022) 2 EJPLT, 8 ff.; L Gatt, "Legal anthropocentrism between nature and technology: the new vulnerability of human beings" (2022) 1 EJPLT, 15 ff.

rights.[13] Its primary interest is to verify the impact of AI systems on human rights in the public and private sectors, by imposing on Member States to guarantee human rights through accurate information, transparency, and independent and effective oversight of technology compliance, but without creating obstacles to the identification of liabilities and remedies in case of the violation of these human rights.

In the same direction, the Council of Europe appointed an ad hoc committee for Artificial Intelligence (CAHAI), in September 2019, that aims to assess the impact of AI on the individual and the society, as well as on existing soft law and hard law instruments that deal with AI. In this light, in December 2020 the CAHAI published a feasibility study that examines,[14] based on broad multi-stakeholder consultations, the potential elements of a legal framework for the development, design and application of AI, based on the Council of Europe standards in the field of human rights, democracy and the rule of law.

Also, the EU initiatives have been developed over the last years, from the European Parliament Resolution on civil law rules on Robotics,[15] until today. The protagonists of the debate are the European Parliament and the European Commission. While the former seemed certain from the outset of the need to intervene to provide specific rules for automation and AI, the European Commission initially considered completely effective the existing regulation also applied to new technologies and then, since 2021, evaluated the possibility of intervening to regulate this phenomenon (AI Act Proposal, AILD Proposal, Proposal for the revision of the PLD [16]).

3. Identification and analysis of tools on the impact of AI.

Recently, there has been a proliferation of self-assessment tools (e.g., ALTAI, 2020; RAII, 2022[17]), AI classification models (e.g., NIST-AI RFM, 2023[18]), and certification programs (such as ISO and IEEE standards; notably the IEEE CertifAIEd program[19]) aimed at evaluating the legal, ethical, and social implications of AI devices and applications. These initiatives translate established ethical and legal principles from various sources (EU AI HLEG, 2019;

[13] Council of Europe, Unboxing artificial intelligence: 10 steps to protect human rights, 2019.
[14] Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility study, 17.12. 2020, CAHAI(2020)23
[15] European Parliament Resolution on Civil Law Rules on Robotics, of 16.02.2017 (2015/2103(INL).
[16] See note no. 10.
[17] High-Level Expert Group on AI (AI HLEG), The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment, 17.07.2020, https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal; Responsible Artificial Intelligence Institute (RAII), The Responsible AI Certification Program. White paper, October 2022, https://www.responsible.ai/how-we-help.
[18] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023, https://doi.org/10.6028/NIST.AI.100-1
[19] IEEE Standard Association, IEEE CertifAIEd certification program, https://engagestandards.ieee.org/ieeecertifaied.html; see also IEEE Standard Association, IEEE 7000™-2021 Standard - Addressing Ethical Concerns During Systems Design, https://engagestandards.ieee.org/ieee-7000-2021-for-systems-design-ethical-concerns.html

OECD, 2019; or NIST[20]) into practical 'checklists', guiding developers and deployers of AI in assessing systems and implementing these principles effectively.

Broadly speaking, the Assessment List for Trustworthy Artificial Intelligence (ALTAI), as the pioneering and most renowned among these tools, along with others, is fundamentally rooted in safeguarding the fundamental rights of individuals, drawing from human rights frameworks embedded in EU Treaties, the Charter of Fundamental Rights, and international human rights law.

Ethics, as delineated by the EU High Expert Group in their 'Ethics guidelines for trustworthy AI',[21] assumes a distinctive role and functionality. Ethical reflection is understood to expand the reach of fundamental rights, functioning both as an argument for (ethically aligned) law interpretation and as an incentive for its voluntary integration, i.e., the voluntary compliance to more stringent ethical standards by developers and deployers of AI systems. This extension aims to steer AI development and use not only towards what is legally permissible, but also towards what is morally imperative, ensuring maximum human well-being.

Furthermore, ethics, from a forward-thinking perspective, should foster the incorporation of ethical values contributing to the attainment of the United Nations' Sustainable Development Goals[22] (UN Agenda 2030[23]). The UN SDGs, encompassing the environmental, economic, and social dimensions of sustainability, provide a crucial paradigm for considering the impact of the development, deployment, and use of AI systems. An AI system should be considered trustworthy (or responsible, as defined in the NIST AI Risk Management Framework[24]) when it not only prioritizes human-centricity but also considers the impact on future generations, respecting the Planet's biophysical conditions and resources, essential and irreplaceable factors for both economic growth and the well-being of humans and the environment.

Consequently, models intended to provide guidance for the ethical and social self-assessment of AI development should consider the growing societal attention to environmental concerns and the increasing preference for an ecological economy, which tends to reward eco-friendly and sustainable development models, as well as responsible consumption practices (a Global Green New Deal[25]). Therefore, AI impact assessment tools should also encompass (and promote) sustainability and ecological responsibility as essential parameters.

This problem is even more significant now, following the very recent approval of the AI Act which, within the framework of (limited) compliance obligations (cf. for example, article 40) and transparency/documentation duties (cf. article 53), or within the scope of voluntary application regulatory

[20] High-Level Expert Group on AI (AI HLEG), Ethics Guidelines for Trustworthy AI, 8.04.2019; OECD, Recommendation of the Council on Artificial Intelligence, 22.05.2019, OECD/LEGAL/0449.
[21] Ethics Guidelines for Trustworthy AI, AI HLEG, cit.; OECD Recommendation of the Council on Artificial Intelligence, cit; AI RMF, NIST, cit.
[22] United Nations, Department of Economic and Social Affairs, Sustainable Development Goals (SDGs), https://sdgs.un.org/goals.
[23] United Nations, General Assembly, Transforming our world: the 2030 Agenda for Sustainable Development, 25.09.2015, A/RES/70/1.
[24] AI RMF, NIST, cit.
[25] J Rifkin, *The Green New Deal* (New York Times, 2019).

tools (e.g., codes of conduct, cf. articles 56, 59), explicitly invokes a principle of sustainable artificial intelligence.

However, a notable gap in most current evaluative tools lies right in the (effective) measurement of AI sustainability, requiring assessments that go beyond mere evaluations of energy consumption or carbon emissions - even though they may extend throughout the entire production cycle and the relevant supply chain, as well as the product lifecycle (see ALTAI, p. 19).

It is crucial, for example, to establish a connection between the ethical and trustworthy (or responsible) "label" associated with AI and the obligation for professionals engaged in AI design, development, or deployment to adhere to organizational practices that align with circular, green, and socially beneficial economies. Standards such as ISO/IEC TR 24368:2022 notably emphasize this aspect.

Moreover, both the production cycle and the utilization of AI products should not only refrain from causing 'significant harm' to the environmental goals (UN 2030 Agenda; EU Green Deal) but also actively contribute to ecological transition, economic and social progress, and the well-being of future generations (cf., e.g., EU Taxonomy Regulation) and, ultimately, the future of AI itself.

The forthcoming interpretations and applications of the AI Act – its compliance obligations and accountability mechanisms (especially the more versatile tools such as the risk management system and the Fundamental rights impact assessment for high-risk AI systems) – present a significant opportunity to actualize societal attention towards sustainability issues and integrate guiding principles for sustainable AI development into regulatory frameworks, thereby safeguarding the interests of current and future generations.

4. First conclusions on how to measure the impact of AI on individuals.

In the previous paragraphs, the possible relationships between law and ethics have been investigated, as well as the current state of the art on the regulation of AIs, and the main existent tools that try to verify the impact of AI. As a result of this research study had been identified the necessary steps to really measure AI's impact on individuals and consequently provide a specific regulation.

Step 1: *How to classify AI based on legal and ethical values – Legal and ethical AI.*

Verification of compliance of AI technology with legal rules and ethical principles, conduct through a measuring tool integrated according to the observations already made, in line with the giuri-ecodinamic approach[26], intended as an ecodynamic analysis of the law or of the legislative policy

[26] PP Franzese, A Riccio, A Scopa, 'Valutazione della sostenibilità ambientale: verso un approccio ecodinamico' (2003) 7 Biologi italiani, 58 ff.

foreseen for the need to not maintain only a legal perspective, since new technologies to be regulated presuppose an interaction between different sciences (from the humanities to the technical sciences). In this way it will be possible to establish the level of AI risk, resulting in differentiated regulation.

Step 2: *Legal and ethical assessment – Lawful AI.*

Specific regulation (legal rules and ethical principles) of AI technologies according to the risk level of AI, with a focus on the main possible issues that may arise from the development of AI (security, privacy, cybersecurity and again ethics).

Step 3: *Empirical analysis – Robust AI.*

Assessment by empirical tests, that should be conducted primarily for high-risk technologies, before they are placed on the market; as well as periodic analysis of the same high-risk technologies after they have been placed on the market.

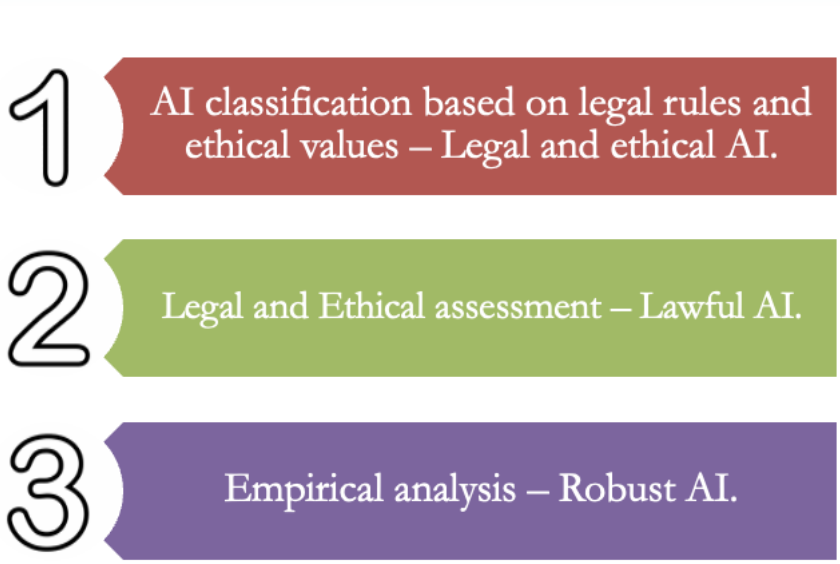


Figure 4: The steps for assessing AI impact on individuals.

Grimaldi P, 'The impact of crytocurrencies on the ecosystem: analysis and possible solutions ' (2023) 2 EJPLT, 121 - 141.
DOI: https://doi.org/10.57230/EJPLT232PG

EJPLT
ISSN 2704-8012



L'impatto delle criptovalute sull'ecosistema: analisi e possibili soluzioni

The impact of cryptocurrencies on the ecosystem: analysis and possible solutions

PAOLA GRIMALDI
RTdA, Professore a contratto di Diritto Privato
Università degli Studi della Campania Luigi Vanvitelli

Abstract

La presente indagine si pone come obiettivo di analizzare l'impatto ambientale delle criptovalute nell'ambito delle iniziative avviate in ambito europeo. Dopo aver delineato un excursus storico delle criptovalute ed illustrato i principali interventi normativi adottati in materia dal legislatore italiano, verrà illustrata la nuova disciplina europea concernente il mercato delle cripto-attività, ovvero il Regolamento MiCA.

The aim of this survey is to analyse the environmental impact of cryptocurrencies as part of the initiatives launched in Europe. After outlining a historical excursus of cryptocurrencies and illustrating the main regulatory interventions adopted on the subject by the Italian legislator, the new European regulation concerning the crypto-asset market, namely the MiCA Regulation, will be illustrated.

© The author(s) 2023, 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: Cripto-attività; Sostenibilità; Blockchain.

Summary: Introduzione. – 1. Le Criptovalute: origini e sviluppo. – 2. Distributed Ledger Technologies (DLT). – 3. Il Regolamento MiCA (UE) 2023/1114 relativo ai mercati delle cripto-attività. – 4. Le altre principali criptovalute: le *Alternative Coin*. – 5. L'impatto ambientale delle criptovalute. – Conclusioni.

Introduzione.

Negli ultimi anni si è assistito ad una rapida crescita e diffusione del mercato delle criptovalute che ha dato esito ad un processo di 'distruzione creativa' e posto l'accento sul tema della questione normativa delle stesse. Difatti, le criptovalute e la tecnologia alla base delle stesse - la blockchain - costituiscono una delle principali innovazioni in grado di cambiare in modo radicale e dirompente il settore finanziario[1]. Le criptovalute hanno dei tratti peculiari che le contraddistinguono dai principali strumenti di pagamento, incorporando diversi benefici e rischi[2]; tra i più discussi e richiamati rischi connessi al settore delle cripto-attività vi sono quello finanziario[3] e quello informatico[4]. Tuttavia, tra i vari rischi legati al fenomeno delle cripto-attività, una particolare attenzione merita l'impatto ambientale delle stesse [5]. In particolare, è necessario considerare i rischi derivanti da tutte quelle cripto-attività che utilizzano meccanismi di consenso particolarmente energivori che si basano sul "Proof-of-work" (PoW) e che, pertanto, richiedono un enorme sforzo computazionale ed un notevole consumo energetico; il Proof-of-Work rappresenta il meccanismo o l'algoritmo di consenso utilizzato dalle principali criptovalute, in primis bitcoin, il cui fine è quello di garantire il funzionamento, la sicurezza e la validazione delle transazioni all'interno della rete, inducendo i miners a competere tra loro per la risoluzione di complessi algoritmi matematici mediante dei processi computazionali altamente energivori. Analizzando, dunque, l'impatto ambientale delle principali criptovalute emergono le criticità delle stesse; la prima di esse è certamente relativa alla circostanza che i sistemi di mining PoW, rispetto ad altri sistemi, quali il Proof-

[1] La nascita delle criptovalute risale convenzionalmente al 2008 quando Satoshi Nakamoto pubblica il *White Paper* intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System",* in cui enuncia i principi teorici e il funzionamento di Bitcoin, evidenziando le potenzialità derivanti dalla creazione di una versione *peer-to-peer* di valuta elettronica totalmente decentralizzata ed indipendente, ovvero fruibile in assenza di un'autorità centrale (quale una banca o un'istituzione finanziaria). Il successo di Bitcoin, ad oggi prima criptovaluta per capitalizzazione di mercato, ha dato luogo alla nascita di numerose criptovalute alternative denominate "*altcoin*".

[2] Sul punto v. R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* in *Diritto dell'informazione e dell'informatica,* XXXII, 1, Milano, 2017, 28.

[3] Connesso principalmente all'elevata volatilità dei prezzi e all'assenza di una regolamentazione. Sul punto vedi G. Arcella, M. Manente, Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza, in *Notariato,* 2020, 23; L. Ammanati, G.L. Greco, *Piattaforme digitali, algoritmi e big data: il caso del credit scoring,* in *Riv. trim. dir. economia,* 2021, 290.

[4] Connesso, ad esempio, a malfunzionamenti tecnologici, all'hackeraggio o al furto delle chiavi crittografiche. Sul punto vedi V. Lauella, *Investire in Bitcoin Strategie, Opportunità e Rischi delle Criptovalute*, Milano, 2023.

[5] G. Falsone, *Crypto e Blockchain*, Tricase, 2022.

of-Stake (PoS), hanno un eccessivo impatto sull'ambiente essendo attività qualificabili come ad alta intensità energetica; in secondo luogo, l'estrazione e la validazione delle criptovalute generano il rilascio di $CO2$ nell'atmosfera; infine, il mining delle criptovalute presuppone l'utilizzo di hardware altamente specializzati soggetti a rapida obsolescenza, nonché dispositivi di raffreddamento che incidono sulla produzione dei rifiuti elettronici e sul problema dello smaltimento degli stessi.

Alla luce di tali premesse, la presente indagine si pone come obiettivo di analizzare l'impatto ambientale delle criptovalute nell'ambito delle iniziative avviate in ambito europeo; in particolare, ai fini della definizione di un quadro complessivo del fenomeno, verrà delineato un *excursus* storico delle criptovalute ed illustrato i principali interventi normativi adottati in materia dal legislatore italiano; verranno evidenziate le criticità connesse all'eccessivo consumo energetico, all'impronta ambientale e al problema dei rifiuti elettrici ed elettronici prodotti; verrà illustrata la nuova disciplina europea concernente il mercato delle cripto-attività, ovvero il Regolamento MiCA che è parte integrante del più ampio pacchetto per la finanza sostenibile adottato dalla Commissione europea

1. Le Criptovalute: origini e sviluppo.

Le nuove tecnologie hanno determinato una trasformazione radicale del tessuto economico, sociale e giuridico tanto da parlare oggi di rivoluzione e/o di era digitale[6]. Le innovazioni tecnologiche sfidano le tradizionali funzioni di intermediazione svolte dalle banche, rivoluzionando diversi settori quale appunto il settore dei mercati finanziari. Si è difatti assistito ad un'evoluzione della moneta e dei sistemi di pagamento che ha indotto l'affermazione di un'economia "*cashless*". Tra queste innovazioni meritano di essere citate proprio le criptovalute[7] - in accezione anglosassone *cryptocurrency* - nonché la *blockchain*, tecnologia alla base delle stesse[8].

Al fine di comprendere il fondamento delle criptovalute, nonché il loro funzionamento, è utile partire dalle origini[9]. Tra i precursori nel settore delle criptovalute ritroviamo David Chaum, noto per i suoi contributi nell'ambito della crittografia [10] , della sicurezza informatica e dell'anonimato delle transazioni digitali; nel 1982 David Chaum, *PhD* in *Computer Science and Business Administration* alla *Berkley University*, pubblicava un paper intitolato "*Blind Signatures for Untraceable Paymentes*" nel quale esprimeva la possibilità di far funzionare un sistema di pagamenti anonimo. Egli presentava, pertanto, un protocollo in grado di garantire la *privacy* delle transazioni finanziarie digitali

[6] M. PETROCELLI, *Incoscienza digitale*, Roma, 2022.
[7] La Banca d'Italia precisa che <<*il termine "valute virtuali" è utilizzato al solo scopo di identificare un fenomeno comunemente noto sotto tale denominazione; l'utilizzo del termine "valuta" non deve pertanto intendersi volto a definire la natura degli strumenti*>>. Consultabile al sito: Banca d'Italia - Avvertenza sull'utilizzo delle cosiddette "valute virtuali" (bancaditalia.it).
[8] C. E. PAPADIMITRIU, *Pagamenti elettronici e nuove tecnologie: profili giuridici,* in *Riv. elettronica dir., econ., management,* 2022, 3, 60.
[9] C. CIANFRONE, *Crittografia e diritto: l'evoluzione storica della crittografia*, in *Ciberspazio e dir., 2*005, 95.
[10] Per una panoramica approfondita sul tema v. C.A. DE ROSA, Sistemi di cifratura. Storia, principi, algoritmi e tecniche di crittografia, Rimini, 2009.

mediante l'utilizzo di *blind signatures*, ovvero una forma di firma digitale in cui il contenuto del messaggio viene nascosto prima di essere firmato[11]. I nuovi sistemi di pagamento elettronico hanno infatti, da un lato, un rilevante impatto sulla *privacy* consentendo, ad esempio, a terzi la conoscenza del proprio stile di vita o delle proprie preferenze, dall'altro soffrono di controlli e sicurezza. Sulla base di questa innovativa idea, nel 1989 Chaum fondò *DigiCash Inc*. e sviluppò "*eCash*". *DigiCash* fu la prima società informatica ad integrare la moneta con la crittografia[12] affinché la stessa potesse essere trasferita senza essere tracciata dalla banca emittente, dal governo o da terzi. Le idee di Chaum sono state poi sviluppate all'interno del movimento di pensiero *cypherpunk*[13] che incoraggiava l'uso della crittografia quale strumento di difesa della *privacy*, considerato come un diritto imprescindibile del gruppo. Nel 1991 Stuart Haber e Scott Stornetta introducevano un prototipo della tecnologia che sarà alla base di *Bitcoin*: la *Blockchain*[14]*;* l'obiettivo era quello di introdurre una tecnologia che consentisse la marcatura temporale dei documenti digitali affinché gli stessi non potessero essere alterati. Nel 1997 il crittografo inglese Adam Back, proponendo un sistema antispam, teorizzava uno dei punti cardine della futura architettura dei *Bitcoin*: la *hashcash proof of work*[15]. Successivamente, nel 1998 Wei Dai, rinomato crittografo e membro della comunità *cypherpunk*, propose *b-money*, una valuta digitale decentralizzata al fine di progettare "un sistema di cassa elettronica distribuito e anonimo". Vennero proposti due protocolli: il primo, sebbene fosse considerato dallo stesso impraticabile, conteneva in sé le basi dell'attuale tecnologia *blockchain* [16] ; il secondo protocollo, invece, introduceva il futuro sistema di verifica di *Bitcoin*. In entrambi i casi, i mittenti e i destinatari sono identificati mediante uno pseudonimo digitale non rintracciabile e ogni messaggio è firmato dal suo mittente e criptato al suo destinatario. Negli stessi anni Nick Szabo teorizzava gli "*smart contract*"[17] e proponeva *Bitgold*, una valuta digitale decentralizzata, che tuttavia non sarà mai concretamente implementata. Infine, un ulteriore contributo fondamentale è dato da Hal Finney, che nel 2004 introduceva un sistema chiamato RPoW (*Reusable Proof Of Work)* attraverso la teoria del *Proof of work,* ovvero l'algoritmo di consenso utilizzato da alcune criptovalute, in particolare *bitcoin*, per validare un blocco di transazioni[18].

L'illustrato background storico, teorico e tecnologico ha condotto Satoshi Nakamoto a presentare alla rete i *Bitcoin*[19].

Dal punto di vista normativo, si ravvisa che il legislatore italiano con il D. Lgs. n. 90 del 2017[20] ha introdotto la lett. qq) nell'art. 1, comma 2, del D. Lgs. n. 231

---

[11] D. CHAUM, *Advances in Cryptology: Proceedings of Crypto 83*, New York, 1984.
[12] F. BRUNTON, *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*, New Jersey, 2019.
[13] Sul punto v. J. CONTER, *Cypherpunk Revolution: a Bitcoin and Blockchain Primer,* USA, 2018; J. Lametta, *Kriptonite. Fuga dal controllo globale. Crittografia, anonimato e privacy nelle reti telematiche*, Torino, 2003.
[14] P. DE NATALE DUMAS, *Privacy e blockchain: quale integrazione possibile?* ,in *Dir. Internet,* 2023, 177.
[15] A. SIMONE, *Bitcoin. L'evoluzione di una rivoluzione*, e-book,Victoria-Canada, 2023.
[16] P. RUBECHINI, *Criptoattività e blockchain,* in *Giornale dir. amm.,* 2023, 263.
[17] G. REMOTTI*, Blockchain smart contract – Un primo inquadramento,* in *Osservatorio dir. civ. e comm.,* 2020, 189.
[18] N. ATTICO, *Blockchain. Guida all'ecosistema. Tecnologia, business, società*, Milano, 2018, 4.
[19] S. NAKAMOTO, *Bitcoin Manifesto*, Milano, 2015.
[20] Recante <<Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante

del 2007[21], meglio noto come Decreto Antiriciclaggio, fornendo una definizione normativa dell'espressione "valuta virtuale" [22] quale <<*rappresentazione digitale di valore, non emessa da una banca centrale o da un'Autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*>>. Definizione poi modificata ed ampliata con il D. Lgs. n.125 del 2019[23], in virtù del quale una valuta virtuale è <<*una rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'Autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*>>. E' possibile individuare alcuni dei principali tratti distintivi delle suddette valute rispetto alle comuni valute a corso legale: le criptovalute non hanno natura fisica ma digitale; una criptovaluta non esiste come moneta cartacea o metallica, ma è una valuta esclusivamente digitale, poiché vengono create, memorizzate ed utilizzate su dispositivi elettronici e conservate in "portafogli elettronici" (i c.d. *wallet*)[24]; le criptovalute sono gestite in maniera decentralizzata considerato che la creazione di nuove unità di valuta e la verifica delle transazioni non dipende da un'autorità centrale ma è gestita direttamente dalla comunità di utenti, a differenza delle monete legali che sono emesse e controllate da una banca centrale o dal governo, come la Banca Centrale Europea (BCE) nell'area dell'euro o la Federal Reserve (FED) negli Stati Uniti; le criptovalute sono generalmente scambiate tra soggetti paritari (*peer-to-peer*): gli scambi avvengono direttamente tra gli utenti senza il ricorso di intermediari; le criptovalute utilizzano la crittografia sia per rendere le transazioni anonime e più sicure, sia per prevenire le truffe; difatti, a tale ultimo proposito, va sottolineato che l'uso della crittografia rende virtualmente impossibile falsificare le transazioni; le transazioni sono tracciabili perchè tutte le transazioni sono registrate sulla *blockchain* e sono pubbliche, sebbene venga garantito il rispetto della *privacy* grazie all'utilizzo di pseudonimi.

Tra i caratteri delle criptovalute, che maggiormente le differenziano da una moneta legale, va evidenziato che esse sono notoriamente volatili poichè i prezzi possono subire ampie fluttuazioni in un breve periodo di tempo; considerata, infatti, l'assenza di una regolamentazione consolidata e l'influenza

---

modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006>>. Su https://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg

[21] Recante <<Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché' della direttiva 2006/70/CE che ne reca misure di esecuzione>>. Su https://www.gazzettaufficiale.it/eli/id/2007/12/14/007X0246/sg

[22] Per un approfondimento delle nuove e delicate problematiche che la valuta virtuale solleva sul piano giuridico, sia per il suo impiego in quanto moneta sia per l'utilizzo come oggetto di investimento, v. M. PASSARETTA, *La valuta virtuale nel sistema dei servizi di pagamento e di investimento*, Bari, 2023. Circa il tentativo fatto dalla dottrina di inquadrarne la natura giuridica v. R. BOCCHINI, *op. cit.*, 31 ss.

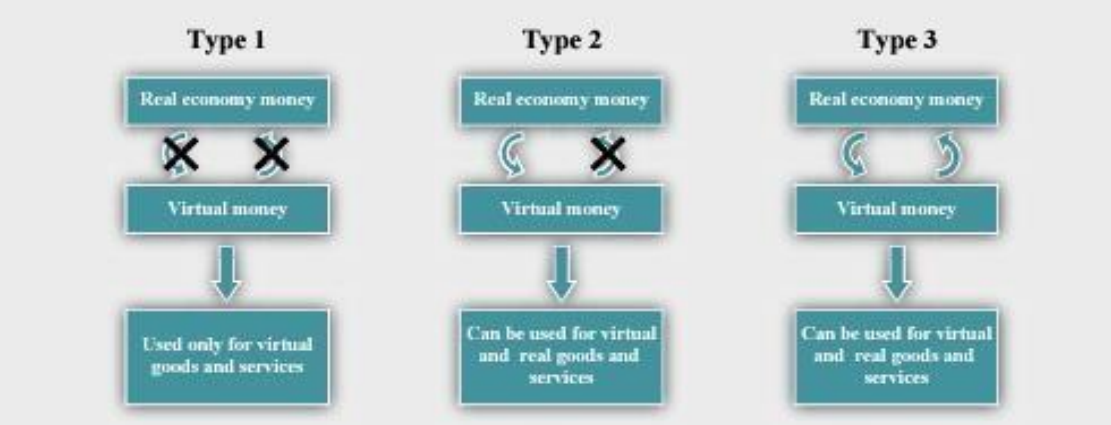
[23] Recante << Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché' attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE>>. https://www.gazzettaufficiale.it/eli/id/2019/10/26/19G00131/sg

[24] G. ARAGUENA, D. JEGERSON, *I pagamenti elettronici. Dal baratto ai portafogli digitali*, Firenze, 2016.

della domanda e dell'offerta, i prezzi delle criptovalute tendono a variare continuamente inducendo gli investitori/risparmiatori ad intravedere nelle criptovalute una opportunità di speculazione. Pertanto, difficilmente, rispetto alla moneta legale, le criptovalute possono essere utilizzate come mezzo di scambio stabile o come riserva di valore. Proprio con riferimento alla funzione di pagamento, si ravvisa che l'art. 1277 c.c. prevede che <<*i debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale*>>; con le criptovalute, non avendo esse corso legale, non vi è alcun dovere giuridico di accettarle per l'estinzione delle obbligazioni pecuniarie, ma possono essere utilizzate per l'acquisto di beni o servizi solo se il venditore è disposto ad accettarle[25].

Dalla suddetta, seppur breve, analisi è possibile iniziare a constatare i vantaggi ed i rischi delle criptovalute. Tra i vantaggi, è riscontrabile, evidentemente, la maggiore autonomia finanziaria garantita dalla disintermediazione o la maggiore tracciabilità e trasparenza delle transazioni, nonché il rispetto della *privacy*. Vantaggi che sono però controbilanciati da diversi rischi, come la già citata volatilità o l'uso delle criptovalute per attività criminali favorite dall'anonimato[26].

Considerati non solo i benefici, ma anche i detti rischi derivanti dall'uso delle criptovalute, e tenuto conto della loro dirompente diffusione, emerge l'esigenza di una regolamentazione comune volta a proteggere gli investitori e a formulare un quadro normativo dedicato certamente più stabile [27]; considerata l'esistenza di una pluralità di criptovalute, la Banca Centrale Europea[28] ha proposto tre modelli fondamentali di criptovalute in base alla loro interazione con l'economia reale:



(Fonte: BCE, Virtual Currency Schemes, 2012).

[25] V. ORSINI, *Della natura giuridica delle criptovalute,* in *Dir. mercato assic. e fin.,* 2021, 15. Per una panoramica completa sul punto si veda, inoltre, I.A. CAGGIANO, *Circolazione del denaro e strumenti di tutela*, Napoli, 2012.
[26] S.M. SCALERA, *Dlt asserviti a scopi illeciti: l'integrazione del reato di riciclaggio tramite l'utilizzo di criptovalute*, in *Antiriciclaggio & compliance,* 2023, 123; N. MAINIERI, N. DI GABIELE, *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli Nft, i*n *www.giurisprudenzapenale.com,* 2022, 6.
[27] M. IRRERA, criptovalute e NFT: il quadro normativo di riferimento, *in Dir. ed economia impr. , 2022, 614.*
[28] EUROPEAN CENTRAL BANK, *Virtual Currency Schemes*, 2012, 13 ss. Consultabile al sito: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

la moneta virtuale chiusa che può essere utilizzata solo all'interno di un determinato sistema o di una determinata piattaforma. Ne sono un esempio le valute dei giochi online[29] che possono essere utilizzate per acquistare oggetti e servizi all'interno del gioco stesso, ma non possono essere scambiate o convertite in valuta reale. La moneta virtuale unidirezionale consente le transazioni soltanto in una direzione, ovvero la valuta virtuale può essere acquistata utilizzando la valuta reale, ma non è possibile riconvertirla nella valuta originale. Tuttavia, mentre con una moneta virtuale chiusa è possibile acquistare solo beni e servizi virtuali, con la moneta virtuale unidirezionale è generalmente possibile acquistare anche beni e servizi reali[30]. La moneta virtuale bidirezionale consente agli utenti di scambiare facilmente la moneta virtuale con la moneta reale e viceversa. Ne sono un esempio i *bitcoin*, che possono essere sia acquistati che venduti in cambio di moneta reale[31]. In particolare, si ravvisa che le criptovalute, secondo quanto previsto dal legislatore europeo nella direttiva 2018/843/UE[32], non sono riconducibili alla categoria delle monete elettroniche[33], in quanto non sono necessariamente legate ad una valuta legalmente istituita[34].

Tra le monete virtuali si annoverano poi i c.d. *stablecoins*, ovvero una forma di criptovaluta che, a differenza delle altre, cerca di mantenere un valore stabile rispetto ad una determinata unità di misura[35]. Pertanto, gli *stablecoins* non presentano la volatilità che contraddistingue normalmente le criptovalute, in quanto il loro valore è legato o a quello di una valuta *fiat* (come il dollaro) o a quello di una *commodity* (come l'oro). Gli *stablecoins*, rispetto alle criptovalute, sono riconducibili alla categoria della moneta elettronica e possono essere considerati degli strumenti di pagamento alternativi alla moneta[36]. Dati i rilevanti sviluppi registrati dai sistemi di valuta virtuale nonché l'esponenziale crescita e diffusione di nuove criptovalute, la Banca Centrale Europea ha poi

---

[29] Sul punto v. D. WOLMAN, *The End of Money. Indagine sul futuro del denaro: avvento e sopravvento di un mondo senza contanti*, Roma, 2015; R. BOCCHINI, *op. cit.*, 36; F. SABRY, *Moneta locale*, Bologna, 2024.

[30] L. DI LORENZO, *L'eredità digitale,* in AA.VV., *Notaio e nuove tecnologie,* 2/2021, Arezzo, 2021.

[31] Per un approfondimento della terminologia di settore cfr. Le criptovalute - EDUCAZIONE FINANZIARIA - CONSOB.

[32] Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE. Consultabile al sito: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018L0843

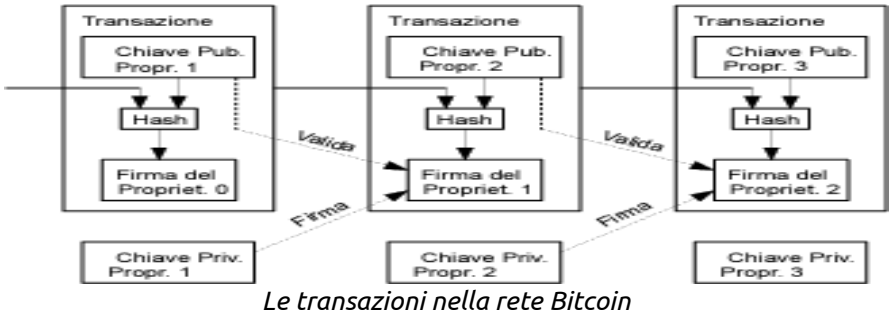
[33] Una prima definizione di "moneta elettronica" è fornita dal legislatore italiano dall'art. 1, co. 2, lett- h- ter), del d.lgs. 1 settembre 1993, n.385, ai sensi del quale, per <<*moneta elettronica*>> si intende: <<*il valore monetario memorizzato elettronicamente, ivi inclusa; la memorizzazione magnetica rappresentato da un credito nei confronti dell'emittenti che sia emesso per effettuare operazioni di pagamento come definite all'art. 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11m e che sia accettato da persone fisiche e giuridiche diverse dall'emittente*>>. Si prevede altresì <<*che non costituisce moneta elettronica: il valore monetario memorizzato sugli strumenti previsti dall'articolo 2, comma 2, lettera m), del decreto legislativo 27 gennaio 2010, n.11; il valore monetario utilizzato per le operazioni di pagamento previste dall'articolo 2, comma 2, lettera n), del decreto legislativo 27 gennaio 2010, n.11*>>. Consultabile al sito: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:1993-09-01;385!vig

[34] A tale conclusione è pervenuta anche la Corte di giustizia, secondo cui "*le valute virtuali sono diverse dalla moneta elettronica come definita dalla direttiva 2009/110/CE, in quanto, a differenza di tale moneta, nel caso delle valute virtuali i fondi non sono espressi nell'unità di calcolo tradizionale, ad esempio in euro, ma nell'unità di calcolo virtuale, ad esempio il 'bitcoin*' " (Corte di Giustizia dell'Unione Europea, Sez. V, Sent. 22/10/2015, n. 264/14).

[35] C.K. ODINET, *The Private Law and Stablecoins*, Arizona, 2022.

[36] A. CINQUE, *La Blockchain. Smart contract, cripto-attività, applicazioni pratiche*, Pisa, 2022, 135ss.

presentato un secondo *report* nel 2015[37] nel quale la BCE stima l'esistenza di circa 500 differenti criptovalute constatando che il numero è in costante crescita. Le criptovalute alternative a *Bitcoin* sono comunemente chiamate '*altcoin*'[38]. Queste monete alternative sono nate per diverse ragioni, come migliorare alcuni punti deboli di *Bitcoin* (ad esempio, migliorare la velocità di convalida delle transazioni), altre, invece, nascono con l'obiettivo di sfruttare la crescente attenzione rivolta dal pubblico a questo fenomeno e pertanto truffare gli investitori[39]. Per quanto concerne la categorizzazione dei diversi tipi di sistema di valuta virtuale, la BCE distingue in primis tra sistemi centralizzati (gestiti e controllati da un soggetto) e sistemi decentralizzati (che si caratterizzano per l'assenza di un emittente e di un amministratore e si fondano sul *peer-to-peer* e su una *blockchain* condivisa, come ad esempio *Bitcoin*), a seconda dell'emissione e del successivo modello di amministrazione. Focalizzando l'attenzione sui sistemi di valuta virtuale decentralizzati, che rappresentano la maggioranza di tutti i modelli, la BCE definisce le diverse categorie nelle quali le criptovalute possono essere raggruppate, in base alle loro caratteristiche e funzionalità. Una prima caratteristica per la quale le criptovalute possono differire sono i sistemi di validazione o algoritmi di consenso, ovvero le modalità utilizzate per validare le transazioni effettuate e mettere in sicurezza la rete; ad esempio, il meccanismo di creazione del consenso utilizzato da *Bitcoin* per la validazione delle transazioni, è noto come *Proof-of-Work* (PoW)[40] e dipende interamente dalla potenza computazionale.



Le transazioni nella rete Bitcoin
*(*Fonte*: Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"*,2008*)*

Un'alternativa che cerca di fronteggiare sia i problemi relativi all'ingente consumo di energia sia la possibilità di manipolazione attraverso un monopolio sul mining è quella del *Proof-of- Stake* (PoS)[41]; in un sistema PoW utenti o gruppi di utenti che controllano il 51% della potenza di calcolo complessiva della rete potrebbero dettare il funzionamento generale del sistema e manipolare le transazioni (questo è noto come l'attacco del 51%). Quindi, a differenza del *Proof-of-Work*, dove l'attività di *mining* è legata alla potenza di calcolo, il *Proof-of-Stake* è legato al numero di unità di valuta posseduta da

[37] EUROPEAN CENTRAL BANK, *Virtual Currency Schemes- a further analysis*, 2015. Consultabile al sito: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
[38] R. GORINI, *Crupto Economy*, Milano, 2022.
[39] E. HARROD, *Altcoin*, California, 2018.
[40] A.BARNINI, A. AGLIETTI, *Bitcoin in action. SegWit, Bitcoin Script & Smart Contracts*, Roma, 2020.
[41] V. BUTERIN, *Proof of Stake The Making of Ethereum and the Philosophy of Blockchains*, New York, 2022.

ciascun utente nella rete. Con il Proof-of-Stake viene pertanto garantita una maggiore efficienza energetica e una maggiore velocità di convalida delle transazioni. Le criptovalute possono poi differire per l'algoritmo utilizzato, ovvero la procedura matematica con la quale si calcolano e si elaborano i dati (ad esempio, l'algoritmo utilizzato da *Bitcoin* è *SHA-256*[42]). Ancora, possono differire, per la quantità di moneta offerta che può essere fissa (come in *Bitcoin*) o flessibile e, ancora, possono differire per le diverse funzionalità[43].

2. Distributed Ledger Technologies (DLT).

Spesso in letteratura si suole indicare i termini *Blockchain* e *Distributed Ledger Technologies* (DLT)[44] come sinonimi, sebbene vi siano invece delle evidenti differenze. Al riguardo, il legislatore italiano ha introdotto il concetto di *Distributed Ledger* nell'ordinamento con il Decreto-legge 135/2018[45], convertito in legge 11 febbraio 2019, n.12.

Ai sensi dell'art. 8-ter, comma 1: *<<si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabile da ciascun partecipante, non alterabili e non modificabili>>*[46].

Nonostante la volontà del legislatore italiano di fornire una base normativa che consenta alle aziende di usufruire della suddetta tecnologia, il primo comma dell'art. 8-ter è stato oggetto di diverse critiche da parte degli esperti in materia, i quali hanno evidenziato il persistente stato di incertezza nonostante l'intervento normativo verificatosi[47]. L'espressione "tecnologie

---

[42] Il termine SHA è l'acronimo di <<*Secure Hash Algorithm*>>. Sul punto v. D. CAPOTI, E. COLACCHI, M. Maggioni, *Bitcoin Revolutio. La moneta digitale alla conquista del mondo*, Milano, 2015, 1-7.

[43] Nonostante le numerose differenze, tutte le criptovalute sono accomunate per la presenza di una pluralità di soggetti che operano nel "sistema"; i principali attori coinvolti sono: gli inventori (*inventors*), ovvero quel soggetto o gruppo organizzato la cui identità può essere nota o sconosciuta (come nel caso di *Bitcoin*) che crea una nuova valuta virtuale, il suo codice e protocollo sottostante e ne sviluppa la parte tecnica; gli emittenti (*issuers*), ovvero coloro che si occupano di generare nuove unità di valuta; I minatori (*miners*), ovvero coloro che volontariamente rendono disponibile la realizzazione dei processi informatici necessari per la convalida delle transazioni, o meglio dei blocchi (un insieme di transazioni è raggruppata in una struttura denominata "blocco"), aggiungendole alla blockchain; gli utenti (*users*), ovvero coloro che decidono di ottenere valuta virtuale per l'acquisto di beni e servizi (virtuali o reali) o per effettuare pagamenti o per scopi di investimento (inclusa la speculazione).

[44] P. OLIVER, *Blockchain 101. Distributed Ledger Technology (Dlt)*, Toronto, 2018.

[45] Decreto-legge 14 dicembre 2018, n. 135 (in Gazzetta Ufficiale - Serie generale - n. 290 del 14 dicembre 2018), coordinato con la legge di conversione 11 febbraio 2019, n. 12, recante: «*Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione*». Consultabile al sito: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazione Gazzetta=2019-02-12&atto.codiceRedazionale=19A00934&elenco30giorni=true

[46] Ai sensi dell'art. 8-ter, al comma 2: *<<si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse (…)>>* e al comma 3 prosegue prevedendo che <<*la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 Luglio 2014*>>.

[47] AA.VV., *La governance delle blockchain e dei sistemi basati sulla tecnologia dei registri distribuiti*, Banca d'Italia, 2023.

basate su registri distribuiti" viene utilizzata dal legislatore come sinonimo del termine "*blockchain*", tralasciando che, in realtà, la *blockchain* è una *species* particolare del *genus* delle *distributed ledger technologies*, ossia delle tecnologie a registro distribuito. La suddetta diversità è appurata anche dalla Risoluzione del Parlamento Europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e *blockchain*[48], laddove si afferma che <<*la blockchain è solo uno dei vari tipi di DLT; che alcune soluzioni DLT memorizzano tutte le singole transazioni in blocchi collegati tra di loro in ordine cronologico per creare una catena che garantisce la sicurezza e l'integrità dei dati*>>. Sostanzialmente, il termine "*Distributed Ledger Technologies"* descrive un particolare tipo di sistema distribuito dove le informazioni possono essere consultate e modificate dagli utenti che partecipano alla rete - c.d. nodi - senza la necessità di una terza parte fiduciaria. È possibile, pertanto, constatare la differenza rispetto ad un sistema centralizzato ove è possibile individuare un'istituzione o controparte centrale nella quale gli utenti ripongono la propria fiducia[49]. Per converso, nei sistemi decentrati, la presenza di un'autorità fiduciaria è sostituita da un meccanismo di consenso distribuito. In particolare si può definire la *blockchain* come un database distribuito che funge da libro mastro o registro delle transazioni e che si fonda su un meccanismo alternativo di fiducia. Si tratta, pertanto, di un particolare *distributed ledger technologies*, in cui il registro è strutturato in 'blocchi concatenati' cronologicamente collegati e controllati e validati dagli utenti del *network*. Per ciascun blocco componente la catena logica, vi è l'indicazione della provenienza e dell'ora di esecuzione attribuita attraverso un meccanismo di crittografia e di marcatura temporale (*timestamping*)[50]. Pertanto, la *blockchain* ha rinnovato il modo di registrare le transazioni e di conservare i dati, garantendo la tracciabilità, la trasparenza e la sicurezza delle transazioni. Si parla, in particolare, di un sistema *trustless*, dal momento che i partecipanti non debbono conoscersi o fidarsi l'uno dell'altro o di un'autorità centrale affinché il sistema funzioni. Una particolare caratteristica della *blockchain* è l'introduzione della "scarsità digitale"[51] poiché la blockchain consente <<*di rendere scarsa l'informazione, dando valore ad un bene immateriale*>>[52]. Grazie all'uso di tecnologie crittografiche, l'asset sarà unico e non replicabile[53].

Al fine di garantire l'adeguamento della disciplina in materia di servizi finanziari all'era digitale, nonché di favorire lo sviluppo di tecnologie

[48] Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP)). Consultabile al sito: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018IP0373

[49] C. GOLA, J. SEDLMEIR, *Addressing the Sustainability of Distributed Ledger Technology*, in *Questioni di Economia e Finanza* (*Occasional Papers*), Banca d'Italia, n.670, 2022, 6. Consultabile al sito: https://www.bancaditalia.it/pubblicazioni/qef/2022-0670/QEF_670_22.pdf?language_id=1

[50] C. PERNICE (2019), *Distributed ledger technology, blockchain e smart contracts: prime regolazioni*, in *InnovazioneDiritto*, 2019. Consultabile al sito: https://www.innovazionediritto.it/distributed-ledger-technology-blockchain-e- smart-contracts-prime-regolazioni.

[51] L'introduzione della c.d. "scarsità digitale" è rilevante anche nell'ambito di *Bitcoin*, dove si è riusciti così a risolvere il problema del *double spending*, consentendo di evitare la duplicazione della moneta ai fini del suo utilizzo per una molteplicità di transazioni. E. GIOVANARDI, D. DE SIMONE, *Siamo tutti non fungibili,* Firenze, 2022, 1-6.

[52] S. SARZANA, F. IPPOLITO, M. NICOTRA, *Diritto della Blockchain, intelligenza artificiale e IoT*, Milano, 2018,18.

[53] C. SANDEI, *L'offerta iniziale di cripto-attività*, Torino, 2022, 3; F. MATTASSOGLIO, *Moneta e tecnologia*, Torino, 2022, 21.

trasformative nel settore finanziario e la diffusione della tecnologia a registro distribuito *(DLT)*, il 30 maggio 2022 è stato approvato il Regolamento 2022/858 (Regolamento DLT) <<*relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE*>>[54].

Con il suddetto Regolamento, all'articolo 2 punto 1), è stata fornita una nuova definizione di tecnologia a registro distribuito (DLT), quale <<*tecnologia che consente il funzionamento e l'uso dei registri distribuiti*>>, ove per registro distribuito, ai sensi dell'articolo 2 punto 2), si intende un <<*archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di noti di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso*>>[55].

Si precisa che il regime pilota relativo alla tecnologia di registro distribuito (DLT) è parte integrante del più ampio pacchetto sulla finanza digitale (*Digitale Finance Package*) adottato dalla Commissione Europea[56].

In conclusione, sul punto, emerge una rilevante attenzione da parte del legislatore europeo, rispetto alle nuove tecnologie e al fenomeno delle cripto-attività, spinto da una necessità di garantire lo sviluppo di un quadro normativo uniforme e stabile, volto a colmare le lacune esistenti nonché garantire un adeguato livello di stabilità finanziaria e di tutela dei consumatori.

3. Il Regolamento MiCA (UE) 2023/1114 relativo ai mercati delle cripto-attività.

Il MiCA (*Market in Crypto-Assets*) costituisce il primo regolamento del mercato delle cripto-attività ed una delle principali applicazioni della tecnologia a registro distribuito (DLT). Approvato il 31 maggio 2023, a conclusione di un percorso lungo e tortuoso avviato nel 2020, è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 9 giugno 2023 introducendo progressivamente le nuove regole al fine di consentire ai singoli Stati membri l'attuazione delle norme nello stesso contenute[57]. In particolare, le norme relative ai *token* collegati ad attività (titolo III) e ai *token* di moneta elettronica (titolo IV) entreranno in vigore a partire dal 30 giugno 2024, mentre

---

[54] Consultabile al sito: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022R0858.

[55] Ai sensi dell'art. 2 punto 3) del Regolamento (UE) 2022/858 per meccanismo di consenso si intendono <<*le regole e le procedure con cui si raggiunge un accordo tra i nodi di rete DLT sulla convalida di un'operazione*>>, ove per nodo di rete DLT, ai sensi dell'art. 2 punto 4), si fa riferimento ad <<*un dispositivo o un'applicazione informatica che è parte di una rete e che detiene una copia completa o parziale delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito*>>.

[56] Il detto pacchetto comprende: a) un regolamento relativo "alla resilienza operativa digitale per il settore finanziario" (*Digital Operational Resilience Act*): il Regolamento DORA (Regolamento (UE) 2022/2554);b) un regolamento relativo ad "un regime pilota per le infrastrutture di mercato basate sulla tecnologia DLT": il Regolamento DLT o Regime Pilota DLT (Regolamento (UE) 2022/858); c) un regolamento "relativo ai mercati delle cripto-attività": il Regolamento MICA (Regolamento (UE) 2023/1114 "*Market in Crypto Asset*"), che mira a regolamentare i *crypto-assets* non qualificabili come "strumenti finanziari" (ai sensi dell'art.4, paragrafo 1, punto 15, della direttiva 2014/65/UE).

[57] A. Filippetta, *Approvato il MiCA: il regolamento (UE) 2023/1114 del 31.5.2023 relativo ai mercati delle cripto-attività* in *www.personaemercato.it,* 2, 2023; C. Boccadutri, *Approvato il Regolamento europeo MiCA sulle criptovalute*, 2023. Consultabile al sito: https://www.boccadutri.com/it/approvato-il-regolamento-europeo-mica-sulle-criptovalute/.

le altre disposizioni si applicheranno dal 30 dicembre 2024[58].

Il Regolamento MiCA è strutturato in nove titoli e 149 articoli e risulta molto ben articolato nei contenuti; esso nasce nell'ambito di un quadro normativo instabile ed inadeguato alla disciplina del mercato delle cripto-attività, a seguito della constatazione del decisivo incremento della capitalizzazione di mercato di alcune criptovalute, che come già ribadito, costituiscono una delle principali applicazioni delle tecnologie di registro distribuito[59]. Il mercato delle cripto- attività, sebbene sia ancora di dimensioni modeste, è in continua crescita favorendo così la nascita e la diffusione di nuovi sottoinsiemi di cripto-attività che presentano disparate caratteristiche. Rilevante è, tra l'altro, anche l'utilizzo e la diffusione delle cripto-attività come mezzo di pagamento in grado di rendere le transazioni più veloci ed efficienti.

Sebbene alcune cripto-attività siano riconducibili alla categoria degli strumenti finanziari e pertanto soggette alla disciplina vigente in materia, altre cripto-attività non sono qualificabili come strumenti finanziari e pertanto sottratte all'ambito di applicazione della legislazione UE in materia di servizi finanziari; queste ultime, non essendo regolamentate, espongono i consumatori, gli investitori ed in generale i possessori a rischi data l'assenza di disposizioni in materia di tutela dei consumatori, protezione degli investitori e di prevenzione di abusi di mercato[60]. Per fronteggiare i rischi appena elencati, alcuni Stati Membri hanno provveduto ad introdurre una propria disciplina sul fenomeno delle cripto-attività, determinando così una frammentazione tra i diversi ordinamenti giuridici in grado di minare la stabilità finanziaria del mercato. Nel descritto contesto, gli obiettivi del Regolamento MiCA possono essere individuati proprio nella volontà di: a) garantire certezza del diritto, ovvero un quadro giuridico solido in relazione al regime applicabile alle cripto-attività non assimilabili alla categoria degli strumenti finanziari, così da consentire uno sviluppo del mercato delle cripto-attività nell'ambito dell'Unione Europea; b) sostenere l'innovazione e la concorrenza leale nell'ambito di un quadro giuridico armonizzato e *ad hoc* per i mercati delle cripto-attività; c) garantire la tutela e la protezione degli investitori e dei consumatori, mitigando e affrontando i rischi a cui gli stessi sono esposti, nonché garantendo l'integrità del mercato, vietando determinati comportamenti quali l'abuso di mercato, l'abuso di informazioni privilegiate, la manipolazione del mercato;; d) garantire la stabilità finanziaria.

Oggetto del MiCA sono le cripto-attività così come definite dall'art. 3, par.1, n.5, <<*rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga*>>. Il legislatore europeo ha volutamente introdotto una definizione di cripto-attività omnicomprensiva del fenomeno al fine di evitare vuoti normativi portati dalla nascita di nuovi sottoinsiemi di cripto-attività. Si tratta, quindi, di rappresentazioni digitali di valore o diritti che possono essere trasferiti e memorizzati su una *blockchain* o su una tecnologia analoga.

---

[58] L'articolo 149 paragrafo 2 prevede l'applicazione del Regolamento dal 30 dicembre 2024; tuttavia il paragrafo 3 prevede altresì che <<*in deroga al paragrafo 2, i titoli III e IV si applicano dal 30 giugno 2024*>>.

[59] P. BONOLIS, G. FLORIO, *La proposta di Regolamento Mica sulle cripto-attività*, 2023. Consultabile al sito https://cms.law/it/ita/publication/la-proposta-di-regolamento-mica-sulle-cripto-attivita.

[60] Per una panoramica approfondita sui rischi derivanti dalla mancanza di tutela legislativa v. R. BOCCHINI, *op. cit.*, 43 ss.

Ancora una volta, con riferimento alla tecnologia, è introdotta una definizione non specifica ma volutamente generica al fine di comprendere tutte le tipologie esistenti (come le *blockchain* centralizzate, decentralizzate, ibride o comunque tecnologie analoghe se fungono da registro distribuito). Pertanto, il termine "tecnologie analoghe" appare ampio e vario, sollevando in molti il naturale interrogativo di quali siano le suddette tecnologie[61].

Con riferimento all'ambito oggettivo di applicazione, il Regolamento in analisi, nel rispetto del principio <<*stesse attività, stessi rischi, stesse norme*>> e al fine di garantire il coordinamento con la normativa del settore finanziario, distingue tra le cripto-attività che non sono qualificate come strumenti finanziari, le cripto-attività assimilabili alla categoria degli strumenti finanziari e le cripto-attività prive di una specifica disciplina. Pertanto, non rientrano nell'ambito di applicazione dello stesso le cripto-attività soggette alla disciplina esistente in materia di servizi finanziari. In particolare, entro il 30 dicembre 2024, l'ESMA dovrà elaborare orientamenti finalizzati a precisare le condizioni e i criteri affinché una cripto-attività possa essere qualificata come uno strumento finanziario (Reg. MiCA, art. 2 par. 5).

Ai sensi dell'articolo 2, par.3, <<*il presente Regolamento non si applica alle cripto-attività che sono uniche e non fungibili con altre cripto-attività*>>, ovvero non si applica con riferimento ai *Non-Fungible-Token* (NFT)[62].

La Commissione per i problemi economici e monetari del Parlamento europeo (ECON), il 14 marzo 2022 ha adottato la propria posizione sulla proposta di Regolamento Mica, pubblicata nel settembre 2020 [63] . Particolarmente interessante, in tale ambito, fu infatti la proposta di inserire nel presente Regolamento degli stringenti requisiti di sostenibilità ambientale con riferimento ai meccanismi di consenso particolarmente energivori quali il PoW, utilizzato *in primis* da *bitcoin*. La proposta sottoponeva i presenti meccanismi di consenso ad un piano di eliminazione, al fine di favorire una graduale transizione verso dei meccanismi di consenso con un minor impatto ambientale e quindi con un minore consumo energetico. A tal fine, alcuni emendamenti del regolamento prevedevano un divieto (o "*ban*") per i prestatori dei servizi relativi alle criptovalute di includere, nella gamma di prodotti offerti, valute non compatibili con i criteri di valutazione ESG.

Pertanto, al fine di raggiungere gli obiettivi climatici ed energetici posti a livello europeo ed enfatizzati nel *Green Deal* europeo, emerge nell'ambito del Regolamento Mica il tema dell'impatto ambientale in connessione con la finalità di disciplinare il settore delle cripto-attività. Difatti, nel considerando 7 del detto Regolamento, la Commissione Europea, prevedendo che i meccanismi di consenso utilizzati dalle principali cripto-attività (*in primis*, meccanismi di consenso PoW) possano avere principali impatti negativi sul clima e sull'ambiente[64], introduce nuovi obblighi in capo agli operatori del mercato di

---

[61] R. VIOLA, L. DE BIASE, *Il codice del futuro. La carta europea dei diritti digitali e il senso dell'innovazione*, Milano, 2023.

[62] C. TREVISI, R.M. VISCONTI, A. CESARETTI, *Non-Fungible Tokens (NFT): business models, legal aspects, and market valuation,* in *Media laws - Riv. dir. media,* 2022, 332.

[63] A. PANTALEO, *Crypto e MiCA: respinto il divieto sul Proof of Work, il meccanismo di consenso di Bitcoin ed Ethereum*, 2022. Consultabile al sito: MiCA: respinto il divieto sul Proof of Work usato da Bitcoin ed Etherum (dirittoaldigitale.com)

[64] Dove si chiarisce che <<*nel determinare se gli impatti negativi sono principali è opportuno tener conto del*

cripto-attività. Si richiama quindi la necessità di mitigare gli impatti negativi derivanti dall'utilizzo di meccanismi di consenso particolarmente energivori mediante il ricorso a delle soluzioni più rispettose per l'ambiente.

4. Le altre principali criptovalute: le *Alternative Coin*.

Si riporta uno schema delle principali criptovalute nella tabella che segue, dove sono ordinate in senso decrescente per capitalizzazione di mercato.

Nome criptovaluta	Prezzo (USD)	Capitalizzazione di mercato (USD)	Unità in circolazione	Volume (24h)
Bitcoin	$30,355.09	$589.790.350.366	19.429.700 BTC	$18.734.837.621 (617.833 BTC)
Ethereum	$1,936.74	$232.799.676.484	120.201.621 ETH	$9.195.669.282 (4.756.061 ETH)
Theter	$1.00	$83.636.493.466	83.613.851.903 USDT	$83.132.958.510 (83.105.902.680 USDT)
BNB	$249.54	$38.889.886.953	155.848.936 BNB	$686.614.812 (2.759.581 BNB)
XRP	$0.727	$38.197.868.914	52.544.091958 XRP	$5.859.609.537 (8.087.339.492 XRP)
USD Coin	$0.9999	$27.282.274.527	27.282.282.461 USDC	$4.302.632.607 (4.302.974.026 USDC)
Cardano	$0.3351	$11.720.930.760	34.976.492.815 ADA	£555.437.134 (1.666.563.557 ADA)

(Elaborazione su dati: https://coinmarketcap.com/it/)

La maggior parte delle suddette criptovalute replicano i meccanismi che sono alla base del funzionamento di Bitcoin; altre, invece, presentano diverse funzionalità ed innovazioni volte a superare i limiti di Bitcoin (come gli alti tempi necessari per la validazione delle transazioni o l'elevata volatilità). Per completezza di esposizione si procede, pertanto, ad una sintetica disamina delle caratteristiche peculiari di alcune delle principali criptovalute in elenco:

- *Ethereum* (Ether): proposta nel 2013 dal programmatore Vitalik Buterin e lanciata nel 2015, rappresenta la seconda criptovaluta per

principio di proporzionalità e delle dimensioni e del volume delle cripto-attività emesse>>.

capitalizzazione di mercato dopo Bitcoin. Si ravvisa che il termine "Ethereum" è utilizzato per indicare la tecnologia mentre l'Ether è la criptovaluta della blockchain Ethereum[65];

- *Tehther* (USDT)[66]: lanciata nel 2014, viene progettata con lo scopo di superare i limiti dettati dall'elevata volatilità delle altre criptovalute. Al fine di garantire la stabilità, i *Tether* sono ancorati al dollaro statunitense; si tratta pertanto di uno *stablecoin*[67].
- *Ripple* (XRP)[68]: XRP è stata ideata nel 2012 da Chris Larsen e Jed McCaleb. A differenza delle altre criptovalute si tratta di una valuta centralizzata controllata dalla società *Ripple*. Altra particolarità è che il *Ledger XRP* (la *blockchain*) non utilizza un meccanismo di consenso *Proof of Work* (come Bitcoin) o *Proof of Stake* (come Ethereum)[69]. Si propone come un'alternativa al sistema SWIFT (acronimo di *Society for Worldwide Interbank Financial Telecommunication*) ed è utilizzata da numerose istituzioni finanziarie e da grandi imprese.

5. L'impatto ambientale delle criptovalute.

Negli ultimi anni si è assistito ad una esponenziale crescita degli investimenti in cripto-attività che ha posto l'accento sul tema dell'impatto ambientale e della effettiva sostenibilità delle stesse[70]. Difatti, nonostante le criptovalute si presentino quali *asset* digitali, questo non vuol dire che siano ad impatto zero. Analizzando il problema dell'impatto ambientale, particolare attenzione meritano tutte quelle cripto-attività che utilizzano meccanismi di consenso che si basano sul *Proof-of-Work*. Il suddetto meccanismo, introdotto per la prima volta con Bitcoin, è ad oggi utilizzato da molte altre criptovalute e si fonda sull'utilizzo delle risorse computazionali per la risoluzione di determinati algoritmi matematici. Difatti, nel caso delle criptovalute come Bitcoin che si basano su tecnologie *blockchain* decentralizzate, il compito di verificare la correttezza e la validità dei blocchi da aggiungere al registro pubblico è affidata agli stessi utenti della rete mediante un processo denominato *mining*. <<*Quando si parla di mining, si intende il processo di condivisione della potenza di calcolo degli hardware partecipanti alla rete*>>[71] volto a verificare la validità delle transazioni e a generare nuove unità di valuta. Per entrambe le operazioni

[65] L'idea alla base di *Ethereum* è di andare oltre il semplice registro delle transazioni, ovvero non consente soltanto l'esecuzione delle transazioni e lo scambio di moneta digitale, ma anche la creazione e distribuzione di applicazioni decentralizzate sulla rete. Per una panoramica d'insieme v. A. HOFFMANN, *Bitcoin ed Ethereum - La Rivoluzione della Nuova Finanza Decentralizzata* (DeFi), Palermo, 2023.
[66] S.A. CHAMBERS, *Money Has No Value*, Berlino, 2023.
[67] I *Tether* erano inizialmente emessi sulla *Blockchain* di Bitcoin utilizzando il protocollo di trasporto "*Omni Layer*"; attualmente, invece, è disponibile su altre *Blockchain*, quale *Ethereum*.
[68] J. GROOM, A. VELLACOTT, *Ripple The big effects of small behaviour changes in business*, Petersfield, 2020.
[69] L'obiettivo principale era quello di ideare una tecnologia che consentisse lo scambio di fondi e l'esecuzione di una pluralità di transazioni a livello globale ed in tempo reale il più velocemente possibile e con bassi costi.
[70] S. D'ALESSANDRO, E. PEDILARCO, *Sustainable Data Gap Earthrise e finanza sostenibile: strumenti finanziari Green e strategia ESG alla luce della normativa europea*, Milano, 2023.
[71] M. PAOLINI, *Bitcoin e mining: qual è il loro impatto ambientale*, 2022. Consultabile al sito: https://quifinanza.it/green/bitcoin-mining-impatto-ambientale/640370/.

i nodi della rete devono risolvere complessi problemi computazionali, altamente energivori, allo scopo di scoraggiare potenziali malintenzionati. La suddetta risoluzione richiede, pertanto, un enorme sforzo computazionale considerato il massiccio consumo di energia. Sebbene un ampio numero di sostenitori della *Proof of Work* abbia individuato nell' elevato consumo di energia richiesto uno dei punti di forza del protocollo, dimostratosi sicuro e resistente agli attacchi, in realtà è proprio focalizzandosi sull'impatto ambientale che emergono le criticità dello stesso. La prima criticità che emerge è legata all'elevato consumo energetico con le connesse emissioni di carbonio e CO_2, aggravata dalla circostanza che i *miners* tendono ad aggregarsi ed a operare in paesi caratterizzati dall' l'elettricità a basso costo e che spesso fanno ancora affidamento su energia a base di carbone, che rappresenta la fonte fossile più inquinante. L'uso di energia da fonti non rinnovabili nel *mining* delle criptovalute contribuisce all'aumento delle emissioni di carbonio e all'effetto serra.

Altro aspetto da considerare è legato alla diffusione delle criptovalute: <<*alla crescita della catena corrisponde un proporzionale aumento nel dispendio di energia e di costi, determinando un allungamento considerevole dei tempi di validazione di ciascun blocco*>>[72]. Sostanzialmente, una maggiore diffusione delle criptovalute comporta un incremento delle transazioni e dell'energia richiesta. Difatti, se inizialmente i problemi matematici erano risolvibili da chiunque fosse in possesso di un computer, attualmente i *miners* sono indotti a creare le c.d. *mining farm o mining pool*, ovvero centri che raccolgono un ampio numero di *miners* e che dispongono di *hardware* altamente specializzati per il *mining* delle criptovalute, nonché di sistemi di raffreddamento essenziali per il contenimento della temperatura dei dispositivi elettronici[73]. Tale sistema impatta sulla produzione di rifiuti elettronici e di conseguenza sull'ambiente, dal momento che l'evoluzione e la diffusione delle criptovalute induce i *miners* a dotarsi di sistemi di calcolo sempre più avanzati con la conseguente precoce obsolescenza dei precedenti *hardware*.

Alla luce delle considerazioni fatte si ravvisa pertanto che, al fine di analizzare l'impatto ambientale delle criptovalute, vi sono diversi fattori da considerare: a) il consumo energetico; b) il *carbon footprint;* c) la produzione di rifiuti elettrici ed elettronici e loro smaltimento.

Per quanto concerne il consumo energetico delle criptovalute, in risposta alle crescenti preoccupazioni sulla sostenibilità e sull'impatto ambientale delle stesse e al fine di quantificare il consumo di energia elettrica nel *mining* a livello mondiale, un team di ricercatori del *Cambridge Centre for Alternative Finance*, ha sviluppato il *Cambridge Bitcoin Electricity Consumption Index* (CBECI)[74], un indice che fornisce stime aggiornate della domanda di energia giornaliera di Bitcoin, nonché una stima del consumo di energia elettrica annualizzato.

Nello specifico il CBECI, al fine di fornire una stima in tempo reale del consumo di energia elettrica della rete Bitcoin, ha adottato una metodologia che si basa su un approccio ibrido *top- down*, sviluppato inizialmente da Marc

[72] A. CINQUE, *La Blockchain. Smart contract, cripto-attività, applicazioni pratiche*, Pisa, 2022, 25.
[73] V. BHATNAGAR, Data Mining in Dynamic Social Networks and Fuzzy Systems, Pennsylvania, 2013.
[74] L. SCHIERA, *Clean air, technology, glocalization, i*n *Sostenibilità globale e culture giuridiche comparate*, Atti del Convegno SIRD Milano 22.4.2022, Milano 2022, 245.

Bevand[75] nel 2017, costruendo un paniere di *hardware* in base al presupposto che i *miners* sono agenti economici razionali e che pertanto utilizzano soltanto *hardware* redditizi.

In particolare, si ravvisa che la domanda effettiva di energia non può essere determinata a causa della natura decentralizzata della rete e pertanto vengono introdotti due limiti: il limite inferiore (*floor*) e il limite superiore (*ceiling*)[76]; entro i due detti limiti è compresa una stima approssimativa ma più accurata della domanda di energia.

Tale modello quindi consente di determinare l'energia elettrica totale consumata dalla rete *Bitcoin*, espressa in gigawatt (GW); questo dato viene aggiornato ogni giorno andando ad indicare la velocità con cui i *miners* consumano elettricità e pertanto consente di descrivere la domanda. Inoltre, viene stimato il consumo annuo di elettricità della rete, espresso in terawattora (TWh).

Lo studio condotto dall'Università di Cambridge ha messo in evidenza come la quantità di energia impiegata per il *mining* di criptovalute sia comparabile al consumo energetico di numerosi Stati. In particolare, ad oggi, si stima che il *mining* di *Bitcoin* abbia richiesto un quantitativo energetico pari a 118.46 TWh, superando il consumo annuale dei Paesi Bassi (113.3 TWh) e delle Filippine (98.5 TWh)[77].

L'analisi sul consumo energetico delle principali criptovalute consente di stimare l'energia elettrica utilizzata dal processo di *mining*; mentre l'analisi dell'impronta ambientale delle criptovalute consente di determinare le implicazioni del processo di *mining*[78].

Difatti, al fine di comprendere l'impatto ambientale delle criptovalute, è necessario correlare i dati ottenuti sui consumi energetici alle diverse fonti di energia che alimentano il processo di *mining* procedendo così a quantificare le emissioni inquinanti. In particolare, dagli studi effettuati dai ricercatori di Cambridge, emerge che, ad oggi, le emissioni di gas serra riconducibili alla rete *Bitcoin* sono pari a 60.96 milioni di tonnellate di anidride carbonica equivalente (MtC02e)[79]. Inoltre, dalla ricerca effettuata è emerso che i *miners* tendono a concentrarsi in quei paesi in cui il clima, le caratteristiche geopolitiche e il costo dell'elettricità agevolano il processo di *mining*[80]*;* difatti è possibile constatare che le *mining farm* tendono a concentrarsi in quei paesi noti per i bassi costi energetici o per il clima freddo che favorisce il raffreddamento delle

---

[75] M.L.PERUGINI, *Distributed Ledger Technologies e sistemi di Blockchain Digital Currency, Smart contract e altre applicazioni*, 2018, 130.

[76] Il limite inferiore rappresenta la domanda di energia teorica minima ed è stimato ipotizzando che i *miners* utilizzino apparecchiature sempre più efficienti dal punto di vista energetico; mentre il limite superiore rappresenta la domanda di energia teorica massima ed è stimato ipotizzando che i *miners* utilizzino sempre le apparecchiature meno efficienti dal punto di vista energetico, fintanto che il funzionamento delle stesse sia ancora redditizio in termini di costi dell'elettricità.

[77] CCAF Digital Tools- *Cambridge Centre for Alternative Finance,* 2023. Consultabile al sito: https://ccaf.io/cbnsi/cbeci/comparisons

[78] R. GORINI, *Crypto economy. Bitcoin, blockchain, DeFi e NFT. Come funziona la nuova economia digitale,* Macerata, 2022.

[79] Bitcoin greenhouse gas emissions, *Cambridge Bitcoin Electricity Consumption Index*, 2023. Consultabile al sito: https://ccaf.io/cbnsi/cbeci/ghg

[80] F. MARZOCCA, *Quanto inquina un bitcoin?*, 2023. Consultabile al sito: https://www.acronico.it/2021/12/17/quanto- inquina-un-bitcoin/.

apparecchiature minerarie funzionanti a pieno regime[81].

In tale contesto, il crescente consumo energetico delle principali criptovalute nonché le preoccupazioni del loro impatto sul clima hanno indotto oltre 250 aziende ed operatori dei settori delle criptovalute, della finanza, della tecnologia, delle ONG e dell'energia e del clima a riunirsi e dar vita al *Crypto Climate Accord* (CCA)[82]. Tale accordo nasce dall'iniziativa di tre organizzazioni quali *Energy Web, Rocky Mountain Institute (RMI) e Alliance for Innovative Regulation (AIR)*, al fine di avviare un'iniziativa, ispirata agli accordi sul clima di Parigi, volta alla decarbonizzazione dell'industria delle criptovalute, dando priorità al clima e sostenendo la transizione dell'intero settore verso emissioni nette di gas serra pari a zero[83]. In particolare, sono stati posti due ambiziosi obiettivi: 1) raggiungere l'azzeramento delle emissioni derivanti dal consumo di energia elettrica entro il 2030 per i firmatari del CCA; 2) sviluppare standard *open source*, strumenti e tecnologie che possano accelerare e favorire lo sviluppo di *blockchain* alimentate al 100% da fonti rinnovabili entro il 2025.

Come anticipato, altro fattore da considerare nell'ambito dell'ampia analisi dell'impatto ambientale delle criptovalute è la rapida obsolescenza degli *hardware* utilizzati per il processo di *mining,* causa di un conseguente aumento dei rifiuti elettronici e di ulteriore consumo di energia necessaria per il raffreddamento dei dispositivi utilizzati.

Nello specifico, nell'ambito dei rifiuti elettronici un problema che si pone è proprio il loro smaltimento[84]. Difatti i RAEE sono caratterizzati da materiali, metalli pesanti e sostanze chimiche che sono altamente tossici – come, ad esempio, il mercurio e il piombo – che penetrando nel suolo e inquinando l'acqua e l'aria possono costituire un danno per l'ambiente e per la salute umana se non gestiti in modo appropriato[85].

Nell'ambito delle criptovalute, in particolare nel caso di *Bitcoin*, il problema dei rifiuti è causato dalla circostanza che, affinché il *mining* sia redditizio, è necessario l'utilizzo di dispositivi sempre più sofisticati, altamente specializzati, con una elevata potenza di calcolo, che pertanto comportano un elevato dispendio energetico che si traduce automaticamente in inquinamento

---

[81] I paesi principali in cui operano i *miner*s di criptovalute includono: gli Stati Uniti (37.84% dell'hashrate totale), la Cina (21.11%) e il Kazakistan (13.22%). La Cina era fino al 2020 la destinazione principale dei *miners* di *Bitcoin* che sfruttavano principalmente l'energia idroelettrica; tuttavia, nel giugno 2021 sono stati emessi divieti al *mining* di criptovalute a causa dell'elevato consumo energetico e la conseguente emissione di carbonio. La decisione del governo cinese ha indotto ad una ridistribuzione geografica dei *miners*. La repressione mineraria in Cina ha determinato una riduzione della quota di energie rinnovabili che alimentano la rete *Bitcoin* dal 41,6% al 25,1%, inducendo i *miners* ad operare in paesi dove l'elettricità si basa principalmente sul gas o sul carbone, quale il Kazakistan, e pertanto aumentando l'impronta di carbonio. In particolare, lo spostamento verso il Kazakistan ha determinato un peggioramento dei risultati dal momento che viene bruciato principalmente carbone fossile, che ha il più alto contenuto di carbonio tra tutti i tipi esistenti. Pertanto, i divieti imposti dalla Cina al *mining* di criptovalute non hanno avuto evidentemente i risultati sperati sulle emissioni di *Bitcoin*. Per una panoramica recente ed approfondita sul tema v. A. DE VRIES, U. GALLERSDORFER, L. KLAABEN, C. STOLL, *Revisiting Bitcoin's carbon foot print*, 2022. Consultabile al link: https://doi.org/10.1016/j.joule.2022.02.005.

[82] L. SCHIERA, *op.cit.,* 246.

[83] *Crypto Climate Accord*. Consultabile al sito: https://cryptoclimate.org/

[84] F. MANNUCCI, *Rifiuti elettronici ed elettrici* in *Riv. guardia di finanza,* 2005, 2073.

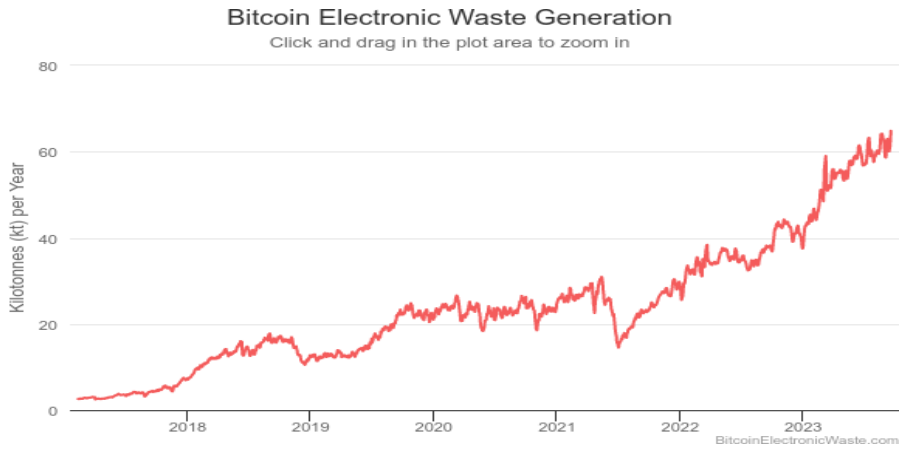
[85] Quando si parla di rifiuti elettronici o RAEE - Rifiuti da Apparecchiature Elettriche ed Elettroniche - si fa riferimento a quei rifiuti derivanti da qualunque apparecchiatura o dispositivo elettrico o elettronico che per il loro funzionamento dipendono da correnti elettriche o da campi elettromagnetici.

ambientale[86].

Altro fattore allarmante da considerare, in virtù delle osservazioni fatte, è che il *mining* richiede l'utilizzo di *hardware* specializzati che, però, hanno una breve vita a causa della forte obsolescenza; i suddetti dispositivi devono pertanto essere continuamente sostituiti ma difficilmente possono essere riutilizzati - proprio a causa della loro alta e settoriale specializzazione - divenendo immediatamente rifiuti. Pertanto, la rete *Bitcoin* non ha solo un problema energetico ma genera anche notevoli quantità di rifiuti elettronici - cd. *e-waste*[87].

È stato creato quindi il *Bitcoin Electronic Waste Monitor* per fornire informazioni sulla quantità di rifiuti elettronici generati dalla rete *Bitcoin*; nello specifico, viene fornita una stima della quantità annuale di rifiuti elettronici prodotti, nonché una stima con riferimento ad una singola transazione.

Su tale ultimo aspetto esaminato, le ricerche e gli studi condotti evidenziano come, al fine risolvere il problema della sostenibilità delle criptovalute, ed in particolare di *bitcoin* quale prima criptovaluta per capitalizzazione di mercato, è necessario non solo ricorrere all'energia rinnovabile ma implementare anche delle politiche volte ad una corretta gestione dei rifiuti elettronici considerato che attualmente, a livello globale, solo il 20% di tutti i rifiuti elettronici viene riciclato, mentre la restante parte finisce in discariche cagionando danni non solo a livello ambientale ma anche per la salute umana[88].



Produzione di rifiuti elettronici in kt/anno (1kt=1000ton)
Fonte: Digiconomist, "Bitcoin Electronic Waste Monitor", https://digiconomist.net/bitcoin-electronic-waste-monitor/

[86] Nel 2009 il *mining* veniva effettuato utilizzando le Unità di Elaborazione Centrale (CPU). Inizialmente, tra l'altro, l'attività di *mining* non era un'attività profittevole dato il prezzo di scambio delle criptovalute; pertanto, i costi dell'energia potevano agevolmente superare il valore dei ricavi. Successivamente le CPU sono state sostituite dalle Unità di Elaborazione Grafica (GPU) che consentono di risolvere più velocemente gli algoritmi crittografici rispetto alle CPU. Ad oggi, le CPU non sono più efficienti per il *mining* delle criptovalute, mentre le GPU sono utilizzate ancora per il *mining* di alcune altcoin. Nel 2012 è stato poi introdotto il *mining* ASIC (acronimo di *Application Specific Integrated Circuit*) ovvero un circuito integrato specifico per determinate applicazioni. Come suggerisce la denominazione, si tratta di dispositivi che sono progettati per uno scopo specifico (ovvero, in questo ambito, per estrarre criptovalute). Quindi con l'ASIC *mining* si fa riferimento ad una modalità di *mining* che prevede l'utilizzo di sistemi ad altre prestazioni conosciuti come ASIC. Sul punto v. M. CALCAGNO, *Cosa è l'ASIC mining e come funziona*, 2021. Consultabile al sito: https://www.hola-cripto.com/corso- criptovalute/cosa-e-asic-mining-e-come-funziona/.

[87] J. LEPAWSKY, *Reassembling Rubbish Worlding Electronic Waste*, Cambridge, 2018.

[88] F. CUMO, A. S. SFERRA, E. PENNACCHIA, *Uso, disuso, riuso*, Milano, 2015, 9.

Conclusioni.

A conclusione di quanto esposto ed indagato fin qui, bisogna chiedersi se le criptovalute possano rappresentare un ostacolo alla realizzazione degli obiettivi generali prefissati, su scala nazionale ed europea, di sviluppo sostenibile e di contrasto al cambiamento climatico. La Banca Centrale Europea (BCE) che è da tempo impegnata nel contrasto dei devastanti effetti del cambiamento climatico, analizzando l'impatto ambientale ed il consumo energetico delle criptovalute e focalizzando la propria attenzione sul *mining* quale possibile ostacolo al raggiungimento degli obiettivi posti a livello europeo verso una transizione verde, ha pubblicato uno studio noto come *Mining the environment- is climate risk priced into crypto-assets?*[89]. Secondo l'indagine della BCE, la crescente diffusione dei *crypto-asset* e la significativa impronta di carbonio degli stessi sta contribuendo a mettere a rischio la transizione verde del settore finanziario.

A questo punto, è necessario chiedersi se le criptovalute e la sostenibilità siano un binomio compatibile, considerando le diverse alternative possibili. Una alternativa certamente più sostenibile è la migrazione verso dei meccanismi di consenso maggiormente rispettosi dell'ambiente, come nel caso di *Ethereum*; iniziativa avviata, nell'ambito dell'acceso dibattito in materia di impatto ambientale, a seguito di numerose critiche da parte della stessa comunità dei *crypto-asset*. Tuttavia, se una parte della comunità dei *crypto-asset* ha raggiunto la consapevolezza della necessità di implementare un cambiamento nel rispetto dell'ambiente, altra parte dei sostenitori delle criptovalute continua a considerare i meccanismi di consenso PoW, maggiormente sicuri, ritenendo che i meccanismi PoS rappresentino una minaccia alla decentralizzazione del sistema. Difatti, nell'ambito dei meccanismi di consenso PoS la sicurezza del sistema è assicurata dalla presunzione che l'utente, che possiede il maggior numero di *asset,* non abbia interesse ad attaccare il sistema stesso ma a validare correttamente le transazioni dal momento che un attacco finirebbe, inevitabilmente, per ledere anche i suoi interessi. Un sistema così implementato può, quindi, mettere a rischio la decentralizzazione inducendo ad un accentramento nelle mani di pochi ossia di coloro che posseggono il maggior numero di *asset*. Proprio in risposta alla necessità di un intervento attivo da parte delle autorità, si collocano le disposizioni contenute nel Regolamento MiCA, in cui sono posti particolari obblighi ai fornitori di servizi di *crypto-asset* al fine di informare correttamente i risparmiatori sui consumi energetici e sugli impatti ambientali delle stesse.

A tal proposito, ci si è chiesti se proprio la categoria degli utenti *inconsapevoli* ed *inesperti* che utilizzano Bitcoin non debba essere tutelata da particolari obblighi informativi[90]; difatti, l'informazione al pubblico delinea un ulteriore fattore chiave nell'ambito della transizione verde, ovvero emerge, con un peso sempre più ampio, il ruolo degli investitori socialmente responsabili e consapevoli, i quali dovranno impegnarsi ad indirizzare i propri capitali in quei

[89] I. GSCHOSSMANN, A.KRAAIJ, P.L. BENOIT, E. ROCHER, *Mining the environment – is climate risk priced into crypto-assets?*, 2022. Consultabile al sito: Mining the environment – is climate risk priced into crypto-assets? (europa.eu).
[90] R. BOCCHINI, *op. cit.*, 44.

crypto-asset in linea con gli obiettivi ESG a cui guardano sempre più settori imprenditoriali.

Attraverso l'analisi condotta nel presente lavoro sui punti di forza e criticità del rapporto tra criptovalute ed esigenze di tutela ambientale, può evidentemente affermarsi che le criptovalute non sono necessariamente incompatibili con la sostenibilità ambientale; al contrario, esse possono offrire dei vantaggi rispetto al sistema bancario tradizionale, che già di per sè ha un impatto ecologico non trascurabile[91].

Le criptovalute costituiscono, dunque, una realtà in continua evoluzione ed innovazione, che presenta delle sfide ma anche delle opportunità per la tutela dell'ambiente e, se da un lato, appare necessario regolamentare e monitorare il loro impatto energetico, dall'altro è certamente possibile sfruttare il loro potenziale per promuovere una transizione verso una economia più verde ed inclusiva. È auspicabile che, anche attraverso l'uso delle criptovalute, opportunamente regolamentate in ogni loro aspetto, si possa contribuire a rendere il settore bancario una industria sostenibile *by* design, un sistema flessibile ed aperto all'innovazione, con un elevato tasso di digitalizzazione; il che vuol dire un minor consumo di carta, una minore mobilità e quindi minori emissioni inquinanti.

[91] Infatti, le banche utilizzano molte risorse materiali, come carta, plastica, metallo, per la produzione e la gestione dei contanti, delle carte di credito, degli sportelli automatici e degli edifici. Inoltre, le banche dipendono da una complessa infrastruttura informatica che richiede energia per funzionare e per mantenersi entro parametri termici precisi. Di tutto interesse sul punto risulta la lettura sul Rapporto ambientale 2023 stilato dalla Banca d'Italia e consultabile al sito Banca d'Italia - Rapporto Ambientale - 2023 (bancaditalia.it).

Trubiani F, 'Cloud computing services : towards a Digital Sustanaibility under EU Digital Law' (2023) 2 EJPLT, 143 - 155.
DOI : https://doi.org/10.57230/EJPLT232TF

EJPLT
ISSN 2704-8012



Cloud Computing Services: towards a Digital Sustainability under EU Digital Law

I servizi di cloud computing: verso la sostenibilità digitale nell'ambito della Strategia Digitale Europea

FRANCO TRUBIANI
Researcher in Private Law
Parthenope University of Naples

Abstract

The contribution aims to investigate, from the perspective of the private law scholar, the complex issue of cloud computing. The author dwells on the potential of this technology not only for the benefit of users and businesses, but also for the service of the public administration in the declared perspective of the search for a sustainable digital environment.
Next, the author analyses, in light of the recent European legal innovations, the main problems, with particular focus on the protection of personal data entrusted to the cloud, trying to hypothesise a new key to interpretation in order to propose new contractual models and reach a renewed responsibility of the cloud service providers.

Il contributo si propone di indagare, dalla prospettiva dello studioso di diritto privato, il complesso tema del cloud computing. L'autore si sofferma sulle potenzialità di questa tecnologia non solo a vantaggio di utenti e imprese, ma anche al servizio della pubblica amministrazione nella dichiarata prospettiva della ricerca di un ambiente digitale sostenibile.
In seguito l'autore analizza, alla luce delle recenti novità legislative europee, le principali problematiche, con particolare riferimento alla protezione dei dati personali affidati al cloud, cercando di ipotizzare una nuova chiave di lettura per proporre nuovi modelli contrattuali e giungere a una rinnovata responsabilità dei fornitori di servizi cloud.

© The author(s) 2023, 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: Digital Sustainability; Cloud services; Technological Innovation; Personal Data.

Summary: 1. Cloud computing as a new technological tool to support digital sustainability. – 2. The 'Cloud First' principle in the Italian National Recovery and Resilience Plan (PNRR). – 3. Cloud Services and EU Law Agenda. – 4. The protection of personal data entrusted to the cloud. – 5. Perspective and Conclusions.

1. Cloud computing as a new technological tool to support digital sustainability.

Cloud computing services, or simply 'cloud', represent the latest model of access to computerized information systems through decentralized computer equipments.[1]

This refers to the on-demand reallocation of access to a shared processing system (such as networks, servers, storage, applications, and services) through which data and functions can be quickly shared.[2]

It is therefore a mode that allows all users to access large computing power without incurring significant economic efforts. This, therefore, requires providers to adapt to computer language, for example, to the standards determined by the owners of cloud distribution platforms.

Such services can be offered jointly by the same provider or, as usual, by different providers; in fact, the network of involved contractual relationships is indicated by the North American doctrine through the image of 'cloud provider contracts chains'.[3]

Often, cloud service providers do not only offer to the end users software applications or, more generally, content, such as music, video or books – or

[1] The Cloud computing market in Italy has reached a value of 3.34 billion euros, an indicator of strong growth contributed to by the health emergency phase that has caused the adoption of cloud in SMEs to rise 42% from a previous year-on-year average of 30% (source: 2020 Report of the Observatory of Digital Transformation, Politecnico di Milano, available at https://www.osservatori.net/it/ricerche/osservatori-attivi/cloud-transformation). According to a Gartner consulting company report published on February 9, 2022, entitled 'Market Impact: Cloud Shift 2022 through 2025,' over the next three years, more than half of Italian corporate spending will shift to the cloud, and already in 2022, with this shift, more than 1.3 trillion dollars of IT corporate spending will be spent, which will grow to almost 1.8 trillion dollars in 2025; this is according to Gartner, compared to 41% in 2022, in three years, 51% of corporate spending, within markets dealing with application software, infrastructure software, business process services, and system infrastructure, will shift from traditional solutions to hybrid and multi-cloud systems.

[2] The National Institute of Standards and Technology (NIST), a division of the US Department of Commerce, established in its 2011 'NIST Definition of Cloud Computing' (available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf) that 'Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models'.

[3] WK Hon, C Millard and I Walden, 'Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now' (2012) 16 *Stan. Tech. L. Rev.* 79, 121, point out that 'several entities may be involved in providing a single cloud service, including suppliers of hardware, software, and data center services. There may be chains of contracts between them. Contractual requirements may vary with the cloud 'stack' component under consideration'.

products sold by the same providers, but also make their platform available to other providers to sell their services (for example in the gaming [4] or entertainment sector [5]), taking advantage of the 'Time to market' factor [6], typical of a net-strategy suitable for technological evolution, through a Lean type process rather than traditional[7], namely, a management style that aims to eliminate waste and to create excellent standardized processes at low cost with the contribution of people.[8]

A peculiar element that characterizes cloud models is the delivery of a service: it is specified, from now on, that this element reveals how the cloud is a model focused not on proprietary size, but precisely on the delivery of computer services by third-party providers, based on a paradigm already widely investigated by economic literature, which in this regard interpreted as a 'new culture of access'.[9]

The increasingly massive use of cloud technology for storing and/or processing data or a complex and integrated service of the indicated features, not only by private individuals but also by public administrations, in the form of the so-called 'community cloud' through which the service is made available to a specific community, represents today a fact that is fully acknowledged and that increasingly leads the interpreter to think about the possible solution of new problems arising from the use of a technical infrastructure whose modes of operation were mostly ignored by the user until few years ago (consumer and non-consumer) and whose activities were subtracted from any regulation.[10]

The European Union itself seems to indicate the study of the legal problems related to the use of cloud computing services in the 'New Consumer Agenda -

[4] Recently, the article M Longan and others, 'Cloud gaming demystified: an introduction to the legal implications of cloud-based video games' (October 27th, 2021), *Queen Mary Law Research Paper*, No. 369/2021, discusses the specific sector of cloud gaming. They propose the existence of a cloud model called Gaming as a Service (GaaS), as a subtype of the Infrastructure as a Service (IaaS) model.

[5] It appears to be clear that having access to cloud distribution platforms represents a key tool for helping to spread and share original works. For more information on this topic, see V Falce, 'Standard e cloud computing' (2015), 29(2) *Dir. ind.*, 155 ff.; ML Montagnani, *Il diritto d'autore nell'era digitale* (Giuffrè 2012) 115 ff.; A Musso, 'La proprietà intellettuale nel futuro della responsabilità sulla rete: un regime speciale?' (2010), 26(6), *Dir. inf.*, 795 ff.; AM Gambino, '*Cloud, diritto d'autore e nuovi modelli di circolazione giuridica*', in *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza* (Giuffrè 2019), 347 ff.; A Bertoni and ML Montagnani, 'La modernizzazione del diritto d'autore e il ruolo degli intermediari internet quali propulsori delle attività creative in rete' (2015), 31(1) *Dir. inf.*, 111.

[6] ME Mcgrath, *Product strategy for High Technology Companies* (McGraw Hill 2001) 55-58.

[7] The references offered by the studies of merchandising sciences seem very useful to understand the utility of the cloud as a tool for companies (and, in particular, for micro-enterprises) in order to accelerate the sales processes and get to the market faster. The compression of response times to the market also makes the company competitive from a strictly economic-financial point of view, since the company could more quickly reach the break-even point, that is, the moment when costs and revenues are balanced and new products begin to generate profit with stable or decreasing investments compared to the launch phase.

[8] But not only that: think about the perspective of the so-called 'cloud robotics', outside the scope of this study, where there is a shift of part of the intelligence of the robot to the cloud through the sharing of information and the abstraction of the hardware used. In the current cloud robotics scenario, the robot is offered almost unlimited computational power in the cloud compared to its real needs. An obvious advantage over the capacity that can be offered by the processing and storage resources on board the machine and, as a result, important functionalities can be performed with a level of accuracy and execution speed that is significantly higher.

[9] The reference obviously goes to J Rifkin, *The age of access* (Penguin 2000).

[10] L Ammannati, '*Il paradigma del consumatore nell'era digitale. Consumatore digitale o digitalizzazione del consumatore?*', in F Capriglione (eds), *Liber Amicorum Guido Alpa* (Cedam 2019), 436.

Strengthening consumer resilience for sustainable recovery' in which the Commission indicated among the new priorities and crucial points of action for the so-called consumer welfare to be worked on until 2025: specifically, point 3.2. of the Agenda, called 'Digital Transformation' aims, in the declared perspective of a development in line with the principles of sustainability and green development, to facilitate the effective right of people to the portability of their data (as widely recognized in the new proposed Data Act Regulation), in the perspective of creating a true single market and European common data spaces.

In this sense, therefore, there is an European trend towards the search for a so-called 'sustainability of the digital environment', that is, the need to build a digital system capable of capturing the potential of technological evolution and, at the same time, of protecting the fundamental rights of individuals.

In the current highly innovative and complex digital context, this investigation aims to analyze, from a strictly civil law point of view, the topic of cloud computing services, focusing in particular on contractual aspects, analyzing the impact that the classification of these services has on our civil code and those related to the responsibility of the cloud service provider, identifying the multiple legal profiles that the use of cloud services entails compared to traditional legal categories in the context of digital sustainability.

2. The 'Cloud First' principle in the Italian National Recovery and Resilience Plan (PNRR).

The Three-Year Plan for Information Technology in Public Administration 2017-2019 approved by the Prime Minister's Decree of 31 May 2017 launched a process of rationalisation and upgrading of the Information and Communication Technology infrastructures of the public administration, based on the technological principle of 'cloud first'.

The aim is to enable administrations to make more efficient and flexible use of Information and Communication Technology resources, with high levels of cost-effectiveness, reliability and security: this is also with a view to fostering the full interoperability of data and an offer of services that is increasingly tailored to the needs of citizens and businesses.[11]

The many legislative interventions aimed at the digital transformation of the Public administrations (P.A.) have created an evolution strategy based on several principles, among which is the so-called 'cloud first'.

According to this principle, P.A. when defining a new project or developing new services one must prioritise the adoption of the cloud paradigm over any other technology.

The qualification process that cloud service providers must undergo involves three main steps: applying for, obtaining and maintaining qualification.

In line with the requirements of the Three-Year Plan, the Digital Italy Agency conducted a census of the Information and Communication Technology assets

[11] G Napolitano, 'Il partenariato pubblico-privato per la realizzazione del Polo strategico nazionale' (2021), 27(6), *Giornale dir. amm.*, 704.

of public administrations, aimed at classifying the relevant infrastructures in terms of reliability and security.[12]

The census, whose results were published as an annex to Agency Resolution No. 1 of 14 June 2019, revealed a picture of high fragmentation, inadequate security levels and high inefficiency in terms of expenditure. Many data center were found to be energy inefficient, obsolete, insecure and wasteful.

In the light of these data, Decree Law No. 76 of 16 July 2020 on 'Urgent measures for digital simplification and innovation' converted into Law n. 120 of 11 September 2020, in order to promote 'the development of a highly reliable infrastructure located throughout the national territory for the rationalization and consolidation of information processing center', provided that central administrations with type B data center, in compliance with the principles of efficiency, effectiveness and cost-effectiveness of administrative action, are obliged to migrate their information processing center and related IT systems to suitable facilities. The latter, therefore, should be identified among: (a) the National Strategic Pole to be set up, (b) infrastructures that already exist and meet the requirements, (c) Sogei's infrastructure, if made compatible with the requirements set forth in the specific regulation of the Cybersecurity Agency or (d) public cloud solutions for non-critical services.

The same Decree-Law No. 76/2020, as further amended by Decree-Law No. 82 of 14 June 2021, converted into Law No. 109 of 4 August 2021, also established that the Cybersecurity Agency, through its own regulation, shall identify the minimum levels of security, processing capacity, energy saving and reliability of digital infrastructures for public administration and define the quality, security, performance and scalability, interoperability and portability characteristics of cloud services for public administration.

The same regulation should further identify the terms and modalities by which the administrations must carry out the aforementioned migrations to technologically suitable structures.

In particular, according to the 'Italian Cloud Strategy' although international practices and technical standards are widely applied by cloud service providers, given the criticality of the data and services involved, the cloud migration strategy cannot disregard a qualification process of public cloud providers and their services. Moreover, qualification should not be limited to assessing the security aspects mentioned above, but also architectural and organisational ones, as these too can affect the resilience of the services provided, e.g. in vendor lock-in situations.

Another important direction, in line with the recent initiatives and directives of the European Digital Agenda, is that of the standardisation, harmonisation and interoperability of cloud services: in this perspective, with the involvement

[12] R Carleo, 'Il futuro della memoria digitale' (2022), 1(1), *La Magistratura*, 1 ff., gives a lucid reflection on the issue of digital data storage, analysing, in particular, the possible problems linked to the new frontier of 'neuromorphic computing' (which should enable machines to learn and think). He concludes his paper by arguing that 'who knows, then, if machines themselves might not become capable of choosing and selecting the data that must be properly stored in time and remembered in digital memory. Hoping for an optimistic view of the developments of artificial intelligence, it is precisely the machines - if they are well programmed to guarantee the purpose of maintaining democratic control over data and also the most appropriate choices on data storage - that could save us from their dictatorship'.

also of Italy, the GAIA-X project was launched at the end of 2019 with the aim of developing common requirements for a European data infrastructure.

The implementation of the National Strategic Pole was therefore included among the qualifying projects of the National Recovery and Resilience Plan transmitted by the Italian Government to the European Commission on 5 May 2021 and, on the latter's proposal, definitively approved by the European Council with the execution decision of 13 July 2021.

Within the measure 'Digitalization, Innovation and Security in the Public Administration' of the NRP, investment 1.1 (Digital Infrastructure) in the amount of EUR 900 million and investment 1.2 (Enabling and Facilitating Migration to the Cloud) in the amount of EUR 1,000 million are planned.

The National Recovery and Resilience Plan (so-called PNRR), therefore, considers cloud computing an essential tool to promote the improvement of IT infrastructures and services of the public administration. The Italian government's declared need is to achieve a proximity cloud in the next few years for at least a couple of reasons: a) there is undoubtedly a technological need (consider for instance of the Internet of Things or Driverless cars) for which it would be more useful for cloud servers to be geographically close to the places of production of the various technological phenomena; b) proximity goes towards realising true digital sustainability in which data are always close to where they are produced, in full respect of the ecological transition & digital sustainability.[13]

3. Cloud Services and EU Law Agenda.

In Europe the first regulatory indications on the cloud date back a few years: in its Communication dated 19th April 2016 on the European Cloud Initiative, the EU Commission pointed out two pillars.

The first pillar is the development of an adequate European infrastructure (European Data Infrastructure), consisting of networks for ultra-fast connectivity and adequate HPC (High Performance Computing) resources.

The second pillar is the provision of European research for a high-quality Cloud system that focuses on the principle of data sharing (European Open Science Cloud – EOSC). If, for the European Data Infrastructure, the issues to be addressed are typical of the infrastructure policy, including the use of European funds and the modalities of private public cooperation, the second pillar deserves a brief analysis – as the process to realize the EOSC is central to the problem of the relationship between new services and protection of rights. The main objective of the EU Commission through the EOSC is to overcome the current fragmentation of databases and the inadequate integer capacity, and facilitate the sharing and reuse of information.

In the current context of the EU Digital Law Strategy there are some provisions that are relevant for Cloud Service Providers. Reference is made in particular to: (a) the General Data Protection Regulation (GDPR), already adopted and in force from 25th May 2018 (which will be discussed specifically

[13] S Epifani, *Sostenibilità digitale. Perché la sostenibilità non può fare a meno della trasformazione digitale* (Digital Transformation Institute 2020).

in the next paragraph); (b) the proposed Regulation on European 'Data Act'[14]; (c) the EU Cybersecurity Strategy (in particular the proposal for a Directive on measures for a high common level of cybersecurity across the EU - NIS2 Directive – Directive 2022/2555/UE on measures for a high common level of cybersecurity across the Union); and (d) some rules on the liability of providers of Internet services (Regulation of the European Parliament and of the Council 2022/2065/EU on a Single Market For Digital Services and amending Directive 2000/31/EC - Digital Services Act) will be included.

With regard to the critical issues related to cloud services, the Proposal 'Data Act' provides for a strengthened right to portability of cloud computing services, facilitating consumers in switching from one cloud data processing service provider to another, preventing vendor lock-in.

On this point, it is envisaged to phase out pass-through tariffs in the three years following the coming into force of the data regulation and, in the medium term, the possibility of introducing a control mechanism on them (Art. 25 Data Act).

The Commission aims to provide a new interoperability framework for the development of common European data spaces; and it does so by empowering European standardization organizations to draft harmonized interoperability standards. This is done with the objective of going beyond the initial EU General Data Protection Regulation (GDPR) approach to personal data portability by extending the remit of this right to non-personal data. This was previously hindered by the lack of important technical specifications – such as for APIs – and by legal language that foresaw interoperability 'only where technically feasible'. Two types of actors are the main targets of such technical requirements: 'operators of data spaces' and 'cloud computing providers'. They will be obliged to enable users' data portability and switchability across digital services.

Finally, Chapter VII touches on the cross-border transfer of non-personal data. The measure, in article 27, compels cloud computing providers to take all reasonable technical, legal and organizational measures, including contractual arrangements to 'prevent international transfer or governmental access to non-personal data held in the Union where such a transfer or access would create a conflict with Union law (…)'.

This means that the Commission will be in charge of developing guidelines consistent with the recommendations of the European Data Innovation Board, to be established under the Data Governance Act (DGA)[15].

At a practical level, the proposed rules for international data transfers have important implications for cloud computing service providers as the Commission is strongly restricting foreign governments' access to non-personal data stored in Europe, unless these are based on international agreements, such as mutual legal assistance treaties.

This seems to be a direct response to the previous controversies sparked by the CLOUD Act, which foresees executive agreements between the US

[14] Please note that the approval by the EU Council's on 27th of November 2023 is subsequent to the date the author sent the article to the Journal's editorial office.

[15] On Data Governance Act see S Tranquilli, 'Il nuovo citoyen européen nell'epoca del Data governance act' (2022), 1-2, *Digital Politics*, 179 ss.

Government and third countries' law enforcement agencies to grant reciprocal access to data held by cloud providers in each other's territories. In the absence of international agreements, the DA allows for transfer of data hosted by cloud computing providers if and only if the third country provides an equitable level of protection to EU law.

If these are met, the minimum amount of data permissible in response to a request shall be transmitted. This is in line with the data transfer regimes stipulated in the GDPR for personal data and the DGA for non-personal data.

The European Commission replaced the NIS Directive, the first piece of EU-wide legislation on cyber security, with the NIS 2 Directive in order to respond to the growing threats posed by digitalisation and the wave of cyber attacks and at the same time strengthen security in companies and supply chains, simplify reporting obligations and introduce stricter supervisory measures and enforcement requirements, including harmonised sanctions throughout the EU.

Compared to the original NIS Directive, NIS2 may expand the number of regulated organizations by 10 times or more. This expansion may lead to new compliance challenges for organizations of all sizes and place additional strain on national cybersecurity authorities tasked with oversight and enforcement.

Companies identified by the Member States as operators of essential services in the above-mentioned areas will have to take appropriate security measures and inform the competent national authorities of serious incidents, e.g. data leaks. Major providers of digital services, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements of the directive.

For example, Art. 23 NIS2 establishes a framework for notifying eligible national authorities and relevant customers of any cyber incident with a significant impact in terms of operational disruption, financial loss, or physical harm. In the event of a significant incident, covered organizations will be required to file an initial report within 24 hours, a requirement that will test their reporting capabilities. Organizations will then be required to file a more detailed report within 72 hours, and a final, comprehensive report within one month.

The Digital Services Act (DSA) included Cloud Service Providers among the recipients of due diligence obligations.

In 'Considerando' n. (13) and n. (28) of the DSA, cloud computing is expressly referred to as an intermediary service included in the Framework. Depending on the concrete operation of the cloud computing service, the rules on exemptions from liability for Cloud Service Providers are the same as for providers of mere conduit, caching or hosting services, which in turn are almost identical to those laid down in Directive 2000/31/EC. Apparently, the only real change that the DSA introduces for the world of cloud computing would be in having made it uncontroversial that a Cloud Service Provider is exempt from liability for what the recipients of the services (its customers) do under the same conditions and with the same exceptions that already applied and will continue to apply, as the case may be, to providers of mere conduit, caching, or information storage services.

Regarding the Internet Service Provide (ISP) liability regime, cloud services must be equated with online platforms[16].

The ISP's liability is excluded if the ISP is not actually aware that the customer's or user's activity (or information) is unlawful and, as far as actions for damages are concerned, is not aware of facts or circumstances that make the unlawfulness of the activity or information apparent (non-knowledge) and if - as soon as it becomes aware of such facts - the ISP acts immediately to remove the information or to disable access to it (timely removal).[17]

In concrete terms, in order to benefit from the limitation of liability, a Cloud Service Providers will have to act immediately to remove the information or to disable access to it as soon as it is informed or becomes aware of the unlawful activities. In addition, it shall take appropriate organisational and technical measures upon being informed, or becoming aware if it has evidence of unlawful activities.

Article 16 of the DSA requires ISPs (including, therefore, Cloud Service Providers) to create mechanisms that enable users to notify the presence of illegal content on their service, and to provide sufficiently precise and adequately reasoned explanations as to why they consider it to be illegal, a clear indication of where it is located, their identification data, and confirmation of their good faith belief in the accuracy and completeness of the information and statements made.

In addition, all ISP's must notify the person or entity issuing the alert of their decision on the information to which the alert relates, providing information on the possibilities for appeal.

Finally, under Article 18 of the DSA, insofar as it qualifies as a hosting provider, even a Cloud Service Provider, if it becomes aware of information that leads to the suspicion that an offence has been committed, is being committed, or is likely to be committed involving a threat to the life or safety of one or more persons, must inform the judicial or law enforcement authorities without delay, providing the available information. Adding together the burden of coping with the reporting and action mechanism governed by Article 16 and the notification of suspected offences under Article 18, it seems clear that the only way for an ISP to be compliant is to equip itself with appropriate procedures, defining roles and responsibilities.

4. The protection of personal data entrusted to the cloud.

A profile of particular relevance to cloud computing concerns the protection of the confidentiality of personal data. The model in question involves the transfer of data, very often generating a cross-border circulation of the same.

[16] The DSA applies to a wide range of intermediary service providers that are classified according to (i) the type of information society service provided and according to (ii) their respective sector and/or size, with special reference to digital platforms.

[17] R Bocchini, '*La responsabilità extracontrattuale del provider*', in R. Bocchini (eds), *Manuale di diritto privato dell'informatica* (Esi 2023), 533 ff.

As it has been correctly pointed out[18], in fact, the distribution model of IT services has been facilitated by the speed of network connections and the ability to aggregate a previously unimaginable amount of computing power in huge data center.

Cloud service providers have data farms located in various parts of the world, managed according to efficiency criteria implying the mobility of the data stored in the 'cloud': these data, in fact, do not reside permanently in the same server, but are continually moved from one server to another due to their optimal allocation, in order to achieve a better management of IT resources.

This process, however, can lead to a breach of confidentiality not only of the personal data of users but also of entire databases of e.g. telephone operators or credit institutions.[19] In the event that a customer makes use of data storage services on the cloud, the risks of an attack or unauthorised access by third parties would multiply, especially in the event that the data transfer is implemented outside European borders.

The need to protect personal data requires the identification of a data controller who is liable for any violations of the General Data Protection Regulation that must receive protection regardless of the territory of the states (art. 3 GDPR).

The problem of the effective application of the protection thus shifts from the difficulty of imposing the legislative rule to that of identifying the data controller, which may not always be easy and immediate to identify.

In fact, in practice, there seems to be a certain distance between the data controller under Art. 4(7) GDPR (usually the client company that relies on a cloud service provider) and the data processor under Art. 4(8) (the cloud service provider): this is because, given that the sector in question is often characterised by the outsourcing of services, which means, in essence, that the longer the cloud 'chain' goes on, the more difficult it becomes for the data controller to ensure compliance with the GDPR.

The growing adoption of networked and distributed architectures, which provide for the compartmentalisation and division of functions relating to data processing, with integrated and competing competences, sees, in fact, the presence of a plurality of data controllers and an integration of their respective competences, often relegating the data controller's function to a more formal than substantial role. The latter, in complex organisations, has the task of defining the purposes of processing and is responsible in the event of unlawful processing, but often lacks effective power of determination and control over the processing methods delegated to third parties.[20]

The flow of data resulting from the provision of cloud computing services can be qualified as a flow between two autonomous data controllers or between a data controller and a data processor. In the first case, the autonomy of the parties' processing would exclude the client's liability for any wrongdoing on the part of the cloud service provider; when, on the other hand,

---

[18] A Mantelero, '*La privacy all'epoca dei big data*' in V Cuffaro, R D'Orazio and V Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli 2019), 1216, nt. 2.

[19] TE Frosini, 'Il costituzionalismo nella società tecnologica' (2021), 36(39, *Dir. inf.*, 474.

[20] A Mantelero, 'GDPR tra novità e discontinuità – Gli autori del trattamento dati: titolare e responsabilità' (2019), 171(12), *Giur. it.*, 2778.

the cloud service provider is considered an autonomous data controller, the client would no longer have any management function in relation to the data processing carried out through the cloud service.

There has been much debate on the legal qualification of the provider, i.e. on whether this contractual figure can be attributed to the role of data controller or data processor.

By virtue of the nature of the professional activity exercised by the cloud service provider, the majority thesis tended to attribute to him the status of processor, i.e. of legal entity entrusted by the customer with the storage of data, as if he were a sort of agent precisely because of the nature of the activity exercised by the cloud service provider.

On the contrary, in B2B relations, the cloud user has the status of controller, i.e. of data controller.

However, on closer inspection, the qualification of the cloud service provider as processor cannot be recognised a priori: this would seem to depend on the margin of bargaining power granted to the cloud user when drawing up the contractual regulation.

In fact, it is possible to resort to the figure of the so-called co-processors provided for in Article 26 GDPR.

Co-processing is established whenever two or more data controllers jointly determine the purposes and means of processing: this is particularly appropriate for the management of cloud computing services where there may be a risk of confusion between the various roles.[21]

The GDPR has intervened to a very marked extent in the definition of the obligations placed on the provider, setting out in Articles 28, 32 and 34 a series of expedients and technical and organisational security measures[22] that each processor is required to adopt so that the data processing offered in the provision of the service can meet the requirements dictated by the same Regulation in order to ensure maximum protection of the rights of the persons concerned by the processing.

The issue of personal data protection becomes even more complex when the data controller, as a professional-businessman, uses cloud services to store personal data of third parties. Indeed, companies and professionals are increasingly relying on cloud technology to manage aspects of their business, outsourcing the storage of documents containing data, including sensitive data, both of their business partners and/or subordinate collaborators, and of their customers.

In this context, therefore, it is the professional client who, in choosing a given service among those available on the web, autonomously defines the

[21] L Valle and Others, '*Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE*' (2018), 18(1), *Contr. impr. Eur.*, 399.

[22] The security measures imposed by the GDPR include: pseudonymisation, encryption of personal data, the ability to ensure the confidentiality, integrity, availability and resilience of systems and services on a permanent basis, and the ability to restore data availability and access in the event of physical or technical disruptions. On this point, the Article 29 Data Protection Working Party of Directive 95/46/EC already expressed its opinion in 2010 (Opinion No. 3 of 2010) that it was necessary to adopt a process aimed at the adoption of legal, organisational and technical measures for the protection of personal data, including through the development of specific organisational models, also aimed at demonstrating that the data processing operations already carried out were carried out in compliance with the European Privacy Regulation then in force.

management modalities and the security regime to which to subject the information in his possession . And if this is the case, then the owner must take care to obtain the consent of the person directly concerned by the processing, even before entrusting such data to the processor or, moreover, to possible subprocessors.

This notwithstanding, if at a theoretical level it is easy to deduce that the burden falls on the controller, in practice it may be difficult for the latter to prepare complete information documents to be submitted to the person directly concerned by the processing, in the absence of the support and cooperation of the cloud service provider.

It should also be noted that, although the possibility of establishing such networks of subprocessors in B2B relations has been recognised, the GDPR, which is designed to protect the personal data of natural persons, mainly places the responsibility on the data controller or, in the cloud context, on the professional client.

The rule can be deduced from a reading of Article 28(1) GDPR, which places an obligation on the data controller to choose only 'data controllers providing sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of this Regulation and ensures the protection of the rights of the data subject', on pain of liability and/or co-liability.[23]

It has been held that the binding nature of the agreement pursuant to Article 28(3) GDPR has a twofold effect on the controller[24]: on the one hand, the controller cannot unilaterally withdraw from the appointment without terminating the main agreement and, on the other hand, the latter cannot legitimately refuse to enter into an act of appointment necessary under the main contractual relationship.

This does not prevent the appointment as controller from having binding effects also vis-à-vis the controller, given that Article 28(3) itself admits the possibility of obligations on the controller.

As regards, instead, the sanctioning profile, Article 82 GDPR has established two forms of liability: one for the controller, as the data controller, who is liable for the damage caused by its processing in breach of the GDPR; the other for the processor, i.e. the data controller, who is liable for the damage caused by the breach of confidentiality in the event of failure to comply with the

[23] On this point, see the decision of the Swedish Data Protection Authority (11 December 2020) - available at https://edpb.europa.eu/news/national-news/2020/university-failed-sufficiently-protect-sensitive-personal-data_it - which fined Umeå University 550,000 Swedish kronor for violating data protection regulations. Specifically, however, no sanction was imposed under the GDPR as the events had occurred before its entry into force. Umeå University, among other violations, allegedly processed special categories of personal data concerning the sexual life and health of its employees by storing them in a cloud storage service of a well-known American company, without designating an appropriate controller. The Swedish Data Protection Supervisor's decision appears relevant as it follows in the footsteps of the well-known 'Schrems II' ruling, arguing that the transfer of personal data contained in cloud storage to the United States would in itself trigger a high risk to personal data as data subjects would be restricted in their ability to assert their rights.

[24] L Bolognini - E Pelino, '*Art. 28. Responsabile del trattamento*', in edited by L Bolognini and E Pelino (eds), *Codice della disciplina privacy* (Giuffrè 2019), 222.

obligations laid down by the GDPR or when it has acted in a manner inconsistent with or contrary to the lawful instructions of the data controller.[25]

In the latter hypothesis, in B2B cloud relationships, the processor is obliged to compensate for damages, including non-pecuniary damages, suffered by the data subject, in addition to being liable for any administrative sanctions imposed by the competent supervisory authorities.

5. Perspective and conclusions.

The impression one gets from these initial introductory remarks on cloud legal issues, observed through the prism of the private law scholar, is that of a topic that appears worthy of further exploration and analysis, given also the speed of technological and legislative evolution.

As correctly acknowledged by an important voice in the current philosophical debate, the advent of the digital 'is changing the conception we have of ourselves'[26] and is going to modify the habits of life of the human being, entailing decisive implications also of a legal nature.

Perhaps, then, the risk that seems to be running is that of preserving an anachronistic law in the face of technological evolution. More specifically, private law itself, through a decisive interaction between the discipline of contracts, the protection of personal data and digital identity, as well as intellectual property, is increasingly being called upon to confront increasingly complex and difficult challenges that continue to call into question its traditional balances.

We can, however, try to make some reflections on the state of the art and possible future prospects.

In addition to the decisive role of European regulation, it seems worth mentioning the importance of the contract for better regulation of cloud computing.[27]

An analysis of commercial practice also reveals the absence of any type of guarantee, the exclusion of liability for damages caused to the user, and the presence of clauses limiting the extent of identifiability for damages caused by the cloud service provider, circumstances that pose delicate problems as to the admissibility of such clauses in our legal system.

The clauses related to the exclusion of liability and limits on identifiability, moreover, are accompanied by the indication that the cloud computing service is normally provided 'as is', in other words 'as available'. The definition of the regulatory regime, in fact, represents a fundamentally important step: the cloud service provider is often located beyond national borders, and user data

[25] N Busca, '*Cloud computing e tutela della privacy nei rapporti commerciali B2B*' (2020), 26(11), *Studium juris*, 1336.

[26] L Floridi, *Il verde e il blu. Idee ingenue per migliorare la politica* (Raffaello Cortina Editore 2020) 77, according to which 'the 'onlife' mode is increasingly underpinning our daily activities. It defines the way we communicate and interact, learn, work, shop, take care of our health, have fun, cultivate our relationships; the way we interact with the legal, financial, political world; even the way we wage war and maintain or promote peace...the digital has changed the way we view ourselves, our world, and our temporality'.

[27] On this point see F Trubiani, '*I contratti di cloud computing: natura, contenuti e qualificazione giuridica*' (2022), 38(2), *Dir. inf*. 395 ff.

are sent, via the network, to systems located in countries whose legal systems provide for a privacy protection regime that is inferior to the European one.

It is therefore necessary to seek to construct a balanced negotiating settlement that allows the customer to have greater certainty.

Since the solutions offered in the area of cloud computing are represented by a wide variety of possible architectures, service models, combination of technologies made available and software adopted, it will be necessary to make explicit in the contract all the assumptions underlying the choice of the solution adopted and the service provider.

Service reliability, authentication and authorisation, cryptography, security incident management and reporting, logging and monitoring, security auditing and verification, vulnerability management and governance of security controls are the main points to be included in an acceptable level of security: the definition of shared technical standards represents the first step in order to accomplish a system of legal rules inspired by and, in a certain sense, able to drive technological development.

An alternative or at least competing scenario, then, could be that of envisaging a form of co-regulation[28], in which the rules are suggested by the market (perhaps through the contribution of the sector's stakeholders, such as the Cloud Security Alliance and of the scholars of new technologies law) and shared by the sector's authorities, following the 'regulatory circle' scheme.[29]

That is, it is a bottom-up mechanism that starts from the market's regulatory drive and introduces rules into the system - or at least immediately operational guidelines - that can then, if necessary, be taken into consideration by the legislator and translated into regulatory precepts.[30]

In the American literature, the development of 'best practices' guidelines is seen as a positive way to effectively regulate these contractual relationships, in particular to facilitate data portability in the cloud[31]: on closer inspection, codes of conduct may also be useful, more generally, to better define the cloud service provider's policy on the retention of users' personal data.

At the end of these considerations, however, the impression is that we are still faced - on the one hand - with a fragmented and still undefined regulatory framework and - on the other - with the need to proceed with the construction of appropriate contractual models for the cloud sector: in this sense, therefore, the role of the interpreter seems important, who will necessarily have to go into the individual issues that have only been hinted at here in greater depth.

---

[28] The term 'co-regulation' is ambiguous by nature. The expression is often used as a generic term to refer to forms of cooperation between market and authorities that are instrumental in the pursuit of regulatory objectives. Co-regulation is generally understood as a form of stakeholder regulation that is promoted, steered, guided or controlled by a third party (be it an official body or an independent regulator) usually endowed with powers of scrutiny, control and, in some cases, sanctioning. On the co-regulation problem see U Malvagna - M Rabitti, 'Filiere produttive e Covid-19: tra rinegoziazione e co-regolazione' (2020) 4(3), *Nuovo dir. civ.*, 369 f.

[29] F Bassan, *Potere dell'algoritmo e resistenza dei mercati in Italia* (Rubbettino 2019).

[30] On the other hand, as recently pointed out by A. Zoppini, *Il diritto privato e i suoi confini* (Il Mulino 2020) 28 f., there are rules and principles (such as those shared in international trade) that impose themselves in private relationships by their own force and that, insofar as they are recognised and shared, perform a normative function independently of their formal adoption.

[31] K Żok, 'Cloud Computing Contracts as Contracts For The Supply Of Digital Content: Classification and Information Duty' (2019), 13(2), *Masaryk University Journal of Law and Technology*, 151.

Montanari Vergallo G, Ricci P, 'L'accertamento del nesso causale nei danni alla persona da inquinamento' (2023) 2 EJPLT, 156 - 168.
DOI: https://doi.org/10.57230/EJPLT232GMVPR
ISSN 2704-8012



L'accertamento del nesso causale nei danni alla persona da inquinamento

The assessment of causation between biological damage and pollution

GIANLUCA MONTANARI VERGALLO
Professore associato di Medicina legale
Università di Roma Sapienza

PASQUALE RICCI
Dottore di ricerca in Medicina sociale e legale
Università di Roma Sapienza

Abstract

La responsabilità civile non ha finora rappresentato un deterrente molto efficace contro l'inquinamento ambientale. Il risarcimento dei danni biologici è spesso impedito dalla difficoltà di dimostrare il nesso causale. Gli autori illustrano lo stato dell'arte della giurisprudenza e la metodologia internazionale di accertamento del nesso causale, così da fornire un chiave di lettura interdisciplinare all'interprete su un tema ad alta stratificazione dottrinale.

Civil liability has not so far represented a very effective deterrent against environmental pollution. Compensation for the resulting biological damage is often prevented by the difficulty of proving causation. The authors clarify the state of the art of jurisprudence and the international methodology for ascertaining causation, so as to provide an interdisciplinary interpretation key to the interpreter on a topic with high doctrinal stratification.

© The author(s) 2023, 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: Nesso causale; inquinamento; metodologia di accertamento.

Summary: 1. Introduzione. – 2. Gli standard probatori della causalità civile. – 3. Causalità generale e individuale. – 4. Conclusioni.

1. Introduzione.

La crescente sensibilità con cui la società civile segue la problematica degli effetti dell'inquinamento sulla salute ha trovato cristallizzazione normativa al più alto livello dell'ordinamento con l'inserimento dell'ambiente in Costituzione all'art. 9, come bene che la Repubblica deve tutelare «anche nell'interesse delle future generazioni» e all'art. 41 come limite alla libertà di iniziativa economica, in virtù della legge costituzionale n. 1/2022. I Costituenti già avevano previsto la sicurezza umana, oltre alla libertà e alla dignità, come contrappeso al valore costituzionale dell'iniziativa economica, così da chiarire che la salute umana non solo non deve essere danneggiata, ma anzi deve essere messa in sicurezza da ciò che la pone in pericolo.

Dal tempo dell'approvazione della Costituzione ad oggi si è assistito a crescenti attività economiche e alla diffusione di stili di vita che, pur senza ledere direttamente la salute, la mettono indirettamente in pericolo (fino a talora danneggiarla) in quanto pregiudicano l'ambiente.

Di conseguenza, la riforma degli artt. 9 e 41 Cost. ben può essere letta come richiamo a proteggere la salute umana non soltanto da danni e da pericoli diretti, ma anche da pericoli indiretti e non necessariamente imminenti, dato l'espresso riferimento, contenuto nel riformato art. 9 Cost., all'obbligo di tutelare le future generazioni.

Il mutamento del quadro di principi sancito in Costituzione non si è ancora riflesso in interventi normativi ed attuativi in grado di migliorare notevolmente la qualità dell'ambiente. Parimenti poco incisiva si è rivelata la mole di disposizioni entrate in vigore nei decenni.

Neppure la Magistratura, nonostante importanti sentenze, ha potuto contribuire ad un cambiamento sistemico di approccio alla protezione dall'inquinamento ambientale, come invece è riuscita a fare nel settore sanitario stimolando, con orientamenti particolarmente severi, pratiche virtuose di gestione del rischio clinico. Tra i problemi che hanno impedito al contenzioso ambientale di esercitare pressione sulle imprese che inquinano e sulle autorità pubbliche tenute al controllo sulle fonti di inquinamento figura la difficoltà di accertare il nesso causale tra la morte o la malattia e l'inquinamento. La soluzione di questo problema porterebbe, attraverso una più effettiva tutela risarcitoria, a meglio attuare l'indicata riforma costituzionale.

2. Gli standard probatori della causalità civile.

Gli standard probatori utilizzati nei processi civili per risarcimento danni nei

Paesi di *common law* possono essere: "*Greater weigh of the evidence*", "*More likely than not*", "*Actual belief*" oppure "*Balance of probabilities*", quest'ultimo usato in Inghilterra e in alcuni Stati del Commonwealth, ma in modo da renderlo sostanzialmente analogo al "*More likely than not*"[1].

Il primo, chiamato anche "*Preponderance of the evidence*", si applica confrontando e soppesando le prove addotte dall'attore e dal convenuto a sostegno delle rispettive conclusioni. Vince la causa la parte che adduce prove preponderanti rispetto a quelle della controparte.

Secondo il criterio del "*More Likely Than Not*", un fatto si considera provato se, dalle complessive prove acquisite nel corso del processo, risulta più probabile che quel fatto sia vero piuttosto che falso. Questo significa stabilire una probabilità superiore a 0,5[2]. Dunque, il "*more likely than not*" si differenzia dalla "*Preponderance of the evidence*" perché il primo non compara la credibilità della tesi del danneggiato con quella del convenuto, ma richiede che la tesi del danneggiato sia più probabilmente vera che falsa[3].

I due modelli sopra indicati possono portare a conclusioni opposte del giudizio. Infatti, le prove addotte dal danneggiato a proprio favore possono essere più numerose di quelle a favore del convenuto, ma l'intrinseca illogicità delle prime può indurre a concludere che quanto sostenuto dal danneggiato è più probabilmente falso che non vero. Infatti, in base al criterio del "*Greater weigh of the evidence*", il danneggiato vince la causa se dimostra che la sua versione dei fatti è più probabile di quella del convenuto. Invece, nel criterio del "*More likely than not*", il danneggiato deve provare che la sua versione dei fatti è più probabilmente vera anziché falsa. Quindi, il livello di probabilità richiesto dal criterio del "*Greater weigh of the evidence*" è più basso di quello corrispondente al "*More likely than not*"[4].

La differenza di esiti applicativi tra i due modelli appare con ancor maggiore evidenza nei casi in cui esistono più spiegazioni causali dell'evento lesivo. In tale ipotesi, il criterio del "*more likely than not*" non muta: la tesi dell'attore dovrà essere più credibile rispetto alla probabilità di tutte le altre spiegazioni causali considerate nel loro insieme, non individualmente[5]. Invece, in base al criterio della "*preponderance of the evidence*", in presenza di più spiegazioni causali, il livello di probabilità necessario per ritenere provato il nesso causale si abbassa: per l'attore è sufficiente che la propria tesi sia più probabile di ciascuna delle altre spiegazioni causali, anche se non abbastanza credibile da risultare più probabile che improbabile[6].

L'"*Actual belief standard*" indica a chi deve decidere la causa (giurati o giudici, a seconda dei sistemi giuridici) di considerare provato un fatto se esiste nella loro mente l'"*Actual belief*" che le prove dimostrano la verità di quel fatto, in

---

[1] J. LEUBSDORF, *The surprising history of the preponderance standard of civil proof*, in *Florida Law Review*, 2015, 67, 1569.

[2] J. LEUBSDORF, *The surprising history of the preponderance standard of civil proof*, cit. Come chiarito da A. FIORI A., *La causalità nelle malattie professionali*, parte II, in *Riv. it. med. leg.*, 2007, 1, 18, l'indicazione di valori percentuali per significare la probabilità logica è arbitrario perché non sono calcolabili con metodo scientifico.

[3] R. BLAIOTTA, *Causalità e colpa: diritto civile e si confrontano*, in *Cass. pen.*, 2009, 49, 78.

[4] J. LEUBSDORF, *The surprising history of the preponderance standard of civil proof*, cit.

[5] FIORI, D. MARCHETTI, *Il più probabile che improbabile ed il più improbabile che probabile*, in *Riv. it. med. leg.*, 2010, 1, 174.

[6] M. TARUFFO, *La prova del nesso causale*, in *Riv. crit. dir. priv.*, 2006, 24, 130.

quanto superano le prove contrarie alla verità di quel fatto.

Anche questo criterio può portare ad esiti applicativi opposti rispetto al "*Greater weigh of the evidence*". Ad esempio, se una sola pubblicazione scientifica sostiene la sussistenza del nesso causale tra un evento e un agente lesivo attraverso ricerche non molto attendibili, ma nessuna dimostra l'insussistenza di tale nesso, il criterio del *Greater weigh of the evidence* dovrebbe portare ad accogliere la domanda risarcitoria, perché non c'è alcuna prova contraria. Ma in base al criterio dell'*Actual belief* si dovrebbe arrivare alla conclusione opposta, perché la scarsa attendibilità dello studio non induce a credere nella sussistenza del nesso causale[7].

Il *belief standard* può essere diverso anche dal *more likely than not standard*. Infatti, si può credere che quanto dichiarato da un testimone o da una pubblicazione scientifica è più probabilmente vero che falso e, al contempo, non sentirsi disposto a dire di "*actually believe*" al testimone o agli autori di quella ricerca[8].

L'attuale quadro giurisprudenziale italiano sembra mettere insieme questi diversi criteri di accertamento elaborati nel *common law*. Infatti, pur a fronte di un'innegabile tendenza ad arginare la discrezionalità del giudice, il principio del prudente apprezzamento del giudice è tuttora vigente, specie nella prova del nesso causale, dove numerosi sono gli aspetti da considerare nell'ambito del giudizio sull'attendibilità delle evidenze. Ad esempio, una metanalisi può essere più attendibile di un'altra perché basata su un maggior numero di studi, ma può al contempo esserlo meno perché elaborata da un gruppo di lavoro meno autorevole o perché ha incontrato meno approvazione nella comunità scientifica. Nessun riferimento giurisprudenziale indica al giudice quale aspetto ritenere più importante degli altri. Quindi, in qualche misura, anche l'ordinamento italiano applica il *belief standard*: la prevalenza quantitativa delle evidenze a favore dell'attore non esime il giudice dal valutarne l'attendibilità e dal rigettare la domanda se risultano inattendibili, ad esempio per palesi limiti metodologici. Ma certamente non accoglie questo criterio fino alle sue estreme conseguenze. Ad esempio, se le evidenze rendono obiettivamente il nesso causale più probabile che non, il giudice non può rigettare la domanda dichiarando di non credere ancora alla tesi dell'attore. La discrezionalità del giudice non può portare a rinnegare le evidenze[9].

La giurisprudenza italiana adotta anche i criteri della *preponderance of the evidence* e del *more likely than not*, ma al riguardo si è assistito ad un'evoluzione. Inizialmente la Suprema Corte usava solo quest'ultima locuzione nella sua

---

[7] J. LEUBSDORF, *The surprising history of the preponderance standard of civil proof*, cit.

[8] J. LEUBSDORF, *The surprising history of the preponderance standard of civil proof*, cit.

[9] Anzi, a partire dalla celebre sentenza Cozzini, la Suprema Corte italiana ha indicato ai giudici di merito cosa esaminare per valutare l'attendibilità di una teoria: «gli studi che la sorreggono. Le basi fattuali sui quali essi sono condotti. L'ampiezza, la rigorosità, l'oggettività della ricerca. Il grado di sostegno che i fatti accordano alla tesi. La discussione critica che ha accompagnato l'elaborazione dello studio, focalizzata sia sui fatti che mettono in discussione l'ipotesi sia sulle diverse opinioni che nel corso della discussione si sono formate. L'attitudine esplicativa dell'elaborazione teorica. Ancora, rileva il grado di consenso che la tesi raccoglie nella comunità scientifica. Infine, dal punto di vista del giudice, che risolve casi ed esamina conflitti aspri, è di preminente rilievo l'identità, l'autorità indiscussa, l'indipendenza del soggetto che gestisce la ricerca, le finalità per le quali si muove», oltre ovviamente «alla qualificazione professionale ed all'indipendenza di giudizio dell'esperto» (Cass. pen., sez. IV, 13.12.2010, n.43786, confermata da Cass. pen., sez. IV, 13 giugno 2019, n. 45935).

formulazione italian[10]. L'espressione *preponderance of the evidence* è comparsa solo successivamente e come equivalente di "più probabile che non"[11]. Dunque, per la Suprema Corte non si tratta di criteri alternativi l'uno all'altro, come invece avviene nel *common law*.

Recentemente, preso atto della loro diversità, la Suprema Corte italiana li ha fusi in un unico metodo, così formulato: "La regola della "prevalenza relativa" della probabilità, rileva - quanto al nesso causale, nel caso di cd. "multifattorialità" nella produzione di un evento dannoso (ovvero quando all'ipotesi, formulata dall'attore, in ordine all'eziologia dell'evento stesso, possano affiancarsene altre) - allorché "sullo stesso fatto esistano diverse ipotesi, ossia diversi enunciati che narrano il fatto in modi diversi, e che queste ipotesi abbiano ricevuto qualche conferma positiva dalle prove acquisite al giudizio", dovendo, invero, essere prese in considerazione "solo le ipotesi che sono risultate "più probabili che non", poiché le ipotesi negative prevalenti non rilevano". Orbene, ricorrendo tale evenienza, vale a dire se "vi sono più enunciati sullo stesso fatto che hanno ricevuto conferma probatoria, la regola della prevalenza relativa" - sempre secondo l'impostazione dottrinaria di cui sopra - "implica che il giudice scelga come "vero" l'enunciato che ha ricevuto il grado relativamente maggiore di conferma sulla base delle prove disponibili"[12]. Dunque, questo metodo sembra doversi svolgere in due fasi: il *more likely than not* si applica nella fase di selezione delle spiegazioni causali da comparare tra loro, mentre la *preponderance of the evidence* consente di decidere il caso.

Sembra possano muoversi obiezioni a quest'approccio. Anche a tacer del fatto che esso assomma le difficoltà ed incertezze applicative dei due modelli[13], non si vede come possano esservi più spiegazioni causali, ognuna delle quali più probabile che improbabile: se una tesi è più probabile che non, le altre spiegazioni causali sono necessariamente più improbabili che probabili. Infatti, nel *common law*, *preponderance of the evidence* e *more likely than not* sono criteri alternativi.

Di conseguenza, il riferimento che la Suprema Corte fa al "più probabile che non" sembra non tanto l'affermazione di un criterio di giudizio quanto un omaggio formale all'esigenza di rigore nell'accertamento della causalità. Di fatto, un antecedente può essere considerato causa anche se l'insieme delle *altre* possibili spiegazioni causali supera il 50% di probabilità logica. Lo conferma la recente giurisprudenza di legittimità, che, in applicazione della massima sopra riportata, ha considerato causa l'antecedente che aveva solo il 30% di probabilità di cagionare l'evento lesivo, in quanto la più credibile

[10] Cass. civ., sez. III, 16.10.2007, n. 21619, in *Resp. civ. prev.*, 2008, 2, 323, con nota di L. LOCATELLI, *Causalità omissiva e responsabilità civile del medico: credibilità razionale o regola del "più probabile che non"?*; G. IADECOLA, *La spiegazione causale "più probabile che non" nelle pronunce della Cassazione: una possibile svolta verso (auspicate) posizioni di maggior equilibrio nella responsabilità civile del medico*, in *Riv.it. med. leg.*, 2010, 6, 849.
[11] Cass. civ., sez. III, 11.06.2009, n. 13530, in *De jure*; Cass. civ., sez. III, 10.11.2015, in *De jure*.
[12] Cass. civ., sez. III, 06.07.2020, n. 13872. Nello stesso senso anche App. Bari, sez. II, 22.06.2022, n. 1011. Consultabile al sito: www.lanuovaproceduracivile.it.
[13] G. MONTANARI VERGALLO, P. FRATI, N.M. DI LUCA., *L'accertamento del nesso eziologico nella responsabilità medica civile tra probabilità e presunzioni*, in *Riv. it. med. leg.*, 2010, 6, 867; G. IADECOLA, *La causalità medica in sede civile: discrasie e problematicità*, in *Riv. it. Med. leg.*, 2007, 3, 573.

spiegazione alternativa non superava il 20%[14]. Ma questo significa che la Suprema Corte ha optato per la *preponderance of the evidence*, non per il *more likely than not*.

3. Causalità generale e individuale.

In Italia come nel *common law*, la prova del nesso causale sia in sede penale che civile presuppone la sussistenza della causalità generale e di quella individuale. La prima consiste nell'idoneità di una certa sostanza a produrre la patologia sofferta dal danneggiato. La seconda sussiste quando quella sostanza ha effettivamente fatto ammalare proprio il soggetto che agisce in giudizio o ai suoi casi se egli è defunto[15]. Infatti, la costante giurisprudenza italiana sostiene che l'accertamento del nesso causale non può essere ancorato esclusivamente alla cd. probabilità quantitativa o statistica della correlazione tra fattore di rischio ed evento lesivo, ma va verificato, secondo la cd. probabilità logica, ossia valutando gli elementi di conferma dell'ipotesi e di esclusione di cause alternative, disponibili in relazione al caso concreto[16].

Nell'accertamento della causalità generale un ruolo di primario rilievo spetta all'epidemiologia. In quest'ambito, una fonte internazionale molto importante è rappresentata dal *Reference Manual on Scientific Evidence*, in quanto si tratta di un testo teorico-pratico elaborato dal *Federal Judicial Center*, agenzia governativa deputata alla ricerca e alla formazione a beneficio dei magistrati statunitensi proprio al fine di fornire loro indirizzi operativi nella gestione di casi civili e penali da decidere in base a prove scientifiche[17].

La metodologia indicata prende le mosse dal c.d. rischio attribuibile, che corrisponde al concetto di rischio relativo, utilizzato in Italia. Si tratta di un dato che indica il rapporto tra l'incidenza di una patologia nei soggetti esposti e quella nei non esposti ad uno stesso fattore di rischio nel medesimo lasso temporale[18]. Se il risultato di questa divisione è pari ad 1, il fattore considerato non influisce sullo sviluppo della malattia. Se è inferiore ad 1, ha un effetto preventivo rispetto all'insorgenza della malattia. Se è pari a 2, gli esposti hanno

---

[14] Cass. civ., sez. III, 26.04.2023, n. 10978, in *IUS Responsabilità civile*, 11 settembre 2023, con nota di D. Zorzit, *Per l'accertamento del nesso causale basta il 30% di probabilità. Riflessioni a margine di una sentenza enigmatica.*

[15] Fiori A., *La causalità nelle malattie professionali*, cit., 14; F. Buzzi, *Causalità* versus *casualità, ovvero: gli effetti nocivi dell'amianto sulle teorie giuridiche*, in *Riv. it. med. leg.*, 2012, 4, 1631; W.O. Dillingham, P.J. Hagan e R.E. Salas, *Blueprint for General Causation Analysis in Toxic Tort Litigation*, in *Fed. N. Def. Corp. Couns.*, 2003, 54, 21.

[16] Cass. civ., 03.01.2017, n. 47; Cass. civ., 08.07.2010, n. 16123; Cass. civ., S.U., 11.01.2008, n. 576; Trib. La Spezia, sez. lav., 10.01.2022, n. 299; Trib. Reggio Emilia, sez. II, 11.04.2016, n. 536, in *De jure*; A. Fiori, *Ipotesi di linea guida per l'accertamento medico-legale del nesso causale*, in *Riv. it. med. leg.*, 2010, 3, 405.

[17] S. Zirulia, *Esposizione a sostanze tossiche e responsabilità penale*, Milano, 2018, 10. Nella letteratura statunitense, si rinvia a M.P. Ram Mohan, E.R. Kini, *Compensation for Environmental Damage: Progressively Casting a Wider Net, but What's the Catch?*, in *Vanderbilt Journal of Transnational Law*, 2021, 54, 611; G.W. Boston, *"A Mass-Exposure Model of Toxic Causation: the Content of Scientific Proof and The Regulatory Experience*, in *Columbia Journal of Environmental Law*, 1993, 18, 181; B.P. Billauer, *The Causal Conundrum: Examining the Medical-Legal Disconnect in Toxic Tort Cases from a Cultural Perspective or How the Law Swallowed the Epidemiologist and Grew Long Legs and a Tail*, in Creighton Law Review, 2018, 51, 1-92.

[18] M.D. Green, M. Freedman, L. Gordis, *Reference guide on epidemiology*, in Federal Judicial Center and National Research Council, *Reference Manual on Scientific Evidence: Third Edition*, 2011, 566 ss.

un rischio doppio rispetto ai non esposti[19].

Come rileva il *Reference Manual*[20], il passaggio dall'osservazione empirica al giudizio di causalità richiede due ulteriori accertamenti. In primo luogo, occorre escludere le tre categorie di errori, ossia il caso, quelli che si verificano nella selezione dei componenti della coorte[21] o nella raccolta delle informazioni, e associazioni indirette in quanto dovute alla presenza di fattori di confondimento[22]. Infatti, l'aumento dell'incidenza della patologia sofferta dall'attore potrebbe essere dovuto non al fattore di rischio di cui si indaga il ruolo causale, ma da una condizione diversa comunemente associata a quel fattore di rischio[23].

In secondo luogo, è necessario valutare la sussistenza dei cc.dd. criteri di *Bradford Hill*[24]. Il nesso causale può sussistere nonostante la mancanza di uno o più criteri, ma occorre un'analisi biologica che spieghi il motivo per cui l'assenza di quel criterio non esclude il nesso causale.

Il primo criterio riguarda la relazione temporale tra malattia ed esposizione al fattore di rischio. Se l'attore è entrato in contatto con il fattore di rischio per un lasso di tempo che, in base alla letteratura scientifica, è troppo breve per generare la malattia, non può sussistere il nesso causale[25].

Il secondo criterio consiste nella forza dell'associazione tra malattia ed esposizione, come cristallizzata nel rischio relativo: quanto più alto è tale dato, tanto più probabile è la sussistenza del nesso causale; tuttavia, anche livelli bassi di rischio relativo non escludono il nesso causale, purché quest'ultimo sia rigorosamente dimostrabile sulla base degli ulteriori criteri[26].

Il terzo criterio indaga l'eventuale relazione dose-risposta: l'incidenza e la gravità della malattia deve essere compatibile con la quantità di esposizione. Tuttavia, non tutti gli agenti causali presentano una relazione dose-risposta.

Il quarto presuppone la conferma dei risultati dopo la replicazione della medesima ricerca su differenti popolazioni e da altri ricercatori[27]. Se ulteriori

---

[19] S. BARBUTI, E. BELLELLI, G.M. FARA, G. GIAMMANCO, *Igiene*, Bologna, 1995, 43 s. Volendo esemplificare, il rischio relativo è pari a 2 quando, nella coorte dei non esposti, si verificano 10 casi ogni 100 soggetti considerati, mentre, nella coorte degli esposti, 20 persone si ammalano ogni 100. Dunque, poiché 10 persone si ammalano pur non essendo esposte al fattore di rischio, il 50% delle malattie tra gli esposti potrebbe essere attribuito al fattore di rischio.

[20] M.D. GREEN, M. FREEDMAN, L. GORDIS, *Reference guide on epidemiology*, cit., 597 ss.

[21] Ad esempio, se i partecipanti allo studio sono eterogenei riguardo ai fattori di rischio collegati alla malattia in esame, il risultato indicherà un rischio relativo che rappresenta solo un rischio medio del gruppo e non un incremento di rischio uniforme ed applicabile ad ogni individuo.

[22] Per gli strumenti utilizzati in epidemiologia al fine di escludere i fattori di confondimento, tra cui *restriction*, *matching*, *randomization*, *crude and adjusted estimates*, *stratification*, *standardization and multivariate analysis*, si rinvia a F. FRANCO, A. DI NAPOLI, *Il confondimento: un bias della stima dell'effetto fra una esposizione ed un esito di salute*, in *Giorn. Tecniche Nefrol. Dial.*, 2018, 30(3-4) 216–218.

[23] S. BARBUTI, E. BELLELLI, G.M. FARA, G. GIAMMANCO, *Igiene*, cit., 46 s.

[24] BRADFORD HILL A., *The environment and disease: association or causation?*, in *Proc R Soc Med.*, 1965, 58, 295–300. Per una parzialmente diversa metodologia si rinvia a M. KUNDI, *Causality and the Interpretation of Epidemiologic Evidence*, in *Environ. Health Perspect.*, 2006, 7, 969–974.

[25] Trib. Milano, sez. lav., 08.05.2019, n. 951, in *De jure*, chiarisce che l'esposizione di un soggetto ad una sostanza (o ad un prodotto) non è comprovata dalla semplice presenza della sostanza stessa nell'aria, ma deve essere verificata dal riscontro di tracce biologiche dell'assorbimento nei liquidi biologici).

[26] Qualcosa di molto simile afferma la costante giurisprudenza, fin da Cass. pen., S.U., 11.09.2001, n. 30328, stabilendo che persino basse percentuali di associazione tra condotta ed evento sono compatibili con la prova del nesso causale prossima alla certezza, se l'istruttoria consente di escludere la sussistenza, nel caso concreto, di spiegazioni causali alternative rispetto alla condotta dell'imputato.

[27] S. BARBUTI, E. BELLELLI, G.M. FARA, G. GIAMMANCO, *Igiene*, cit., 47, qualificano questo criterio come "consistenza dell'associazione".

ricerche portano a risultati incoerenti rispetto a quelli iniziali, ciò non esclude automaticamente il nesso causale. Tuttavia, per raggiungere la prova del nesso, diventa necessario dimostrare che i differenti risultati dipendono da motivi che rendono quelle ricerche non abbastanza pertinenti al caso in esame[28].

Il quinto criterio richiede di indagare se l'associazione tra malattia ed esposizione sia coerente con le conoscenze scientifiche attuali. Quanto meno è conosciuto il meccanismo di una malattia, tanto +meno questo criterio può essere determinante. Tuttavia, l'incoerenza tra l'osservazione e le conoscenze biologiche, pur non escludendo di per sé il nesso causale, rende necessario che l'osservazione trovi conferma in altri studi.

Logicamente conseguente a questo criterio è quello che verifica la coerenza tra l'associazione e le ulteriori conoscenze rilevanti, ossia diverse da quelle scientifico-biologiche. Ad esempio, sarebbe incoerente riscontrare un aumento di mortalità per tumore al polmone ed una diminuzione di vendite delle sigarette. Per ottenere l'accoglimento della domanda risarcitoria diventa necessario spiegare che tale incoerenza è dovuta a motivi che non rendono improbabile il nesso causale.

Il settimo criterio studia gli effetti della cessazione dell'esposizione. Spesso mancano dati che consentano di indagare quest'aspetto. Tuttavia, quando è possibile dimostrare che l'eliminazione dell'esposizione riduce l'incidenza della malattia, questo rappresenta un forte elemento di conferma della causalità generale.

Infine, occorre considerare la specificità, ossia la correlazione tra esposizione ed una singola malattia o tipo di malattia. Quanto maggiore è il numero di malattie cui è associato un agente, tanto più difficile è dimostrare il nesso causale. Tuttavia, come già visto per gli altri criteri, neppure la mancanza di specificità impedisce in ogni caso di ritenere provato il nesso causale, purché sia ben giustificata con argomenti scientifici. Ad esempio, il fumo di sigarette è associato a molte e differenti malattie, ma ciò non esclude la sua correlazione causale con il tumore del polmone. Infatti, tale varietà di malattie si spiega alla luce della molteplicità di agenti pericolosi presenti nelle sigarette[29].

Il passaggio dalla causalità generale a quella individuale richiede una doppia indagine, anch'essa indicata dal *Reference Manual*. In primo luogo, è necessario verificare che il danneggiato e le persone sottoposte allo studio presentino caratteristiche simili, anche con riferimento al tempo di latenza e ad altri fattori di rischio[30]. Ad esempio, i risultati dello studio possono essere inidonei a dimostrare il nesso causale se l'età del danneggiato è maggiore rispetto a

---

[28] Anche la Suprema Corte italiana non applica questo criterio in modo rigido: non è indispensabile che la legge scientifica sia accreditata presso la comunità scientifica internazionale, potendo anche trattarsi di una teoria esplicativa nuova o comunque originale, purché «*ciascuna delle assunzioni a base della teoria* [...] *sia verificabile e verificata secondo gli ordinari indici di controllo della attendibilità scientifica di essa e dell'affidabilità dell'esperto*», ossia secondo i sopra riportati criteri stabiliti dalla sentenza Cozzini (Cass. pen., sez. IV, 13.06.2019, n. 45935. Consultabile al sito: https://www.sistemapenale.it/it/scheda/cass-45935-del-2019-amianto-effetto-acceleratore-criteri-selezione-scienza-nuova).

[29] M.D. GREEN, M. FREEDMAN, L. GORDIS, *Reference guide on epidemiology*, cit., 606.

[30] Come rilevano G.A. NORELLI, M. FOCARDI, *Causalità e malattie professionali*, in *Riv. it. med. leg.*, 2015, 4, 1450, per stabilire se il fattore di rischio ha causato o concausato la malattia, occorre valutare la durata (criterio cronologico), l'intensità (criterio di adeguatezza lesiva) e le modalità (criterio topografico e modale) dell'esposizione.

quella dei partecipanti allo studio e tale da giustificare di per sé l'insorgenza della malattia oppure è stato esposto ad una dose minore rispetto a quella utilizzata nello studio[31].

La similitudine tra danneggiato e partecipanti allo studio non è sufficiente a passare dalla causalità generale a quella individuale: non dimostra che, nel caso concreto, l'agente patogeno ha causato la malattia. Infatti, nonostante questa similitudine, si verifica che: *a*) non tutti gli esposti all'agente patogeno si ammalano; *b*) altre persone contraggono la stessa malattia pur non essendo esposte a quell'agente patogeno.

Per arrivare alla prova della causalità individuale occorre una seconda indagine (c.d. esclusione dei decorsi causali alternativi), che porti ad escludere, nel caso concreto, che: *a*) un fattore di rischio diverso dall'agente patogeno abbia causato autonomamente la malattia più probabilmente dell'agente patogeno (se si segue il criterio della *preponderance of the evidence*), oppure *b*) l'agente patogeno risulti essere causa meno probabile rispetto agli altri fattori di rischio, considerati non individualmente ma nel loro insieme, ossia sommando la probabilità logica di ciascun fattore (se si segue il criterio del *more likely than not*)[32].

La Suprema Corte italiana, come pure la giurisprudenza statunitense[33], attribuisce particolare rilevanza probatoria all'esclusione dei decorsi causali alternativi. Infatti, anche a fronte di bassi livelli di probabilità statistica, il giudice può ritenere provato il nesso causale con elevato grado di credibilità razionale se è possibile escludere con certezza le altre possibili spiegazioni

---

[31] Cass. civ., sez. lav., 12.10.2012, n. 17438, in *Riv. it. med. leg. dir. san.*, 2013, 3, 1552, nel respingere il ricorso per l'annullamento della sentenza d'appello, rileva che il c.t.u. ha ritenuto più rilevanti gli studi che avevano preso in considerazione elementi più corrispondenti a quelli del caso concreto.

[32] F. Piraino, *Causalità e responsabilità contrattuale (tenzone tra un giudice e un professore).* Parte I: *La causalità generale*, in *Foro it.*, 2022, V, 266; C. Viazzi, *L'accertamento del nesso causale: ruolo della medicina legale e ricostruzione giuridica del fatto*, in *Riv. it. med. leg.*, 2012, 1, 33; M. Trashaj, *La responsabilità del medico di Pronto Soccorso e la tutela del paziente a partire da un caso di difficile accertamento della causalità individuale*, in *Riv. it. med. leg.*, 2022, 1, 192. Al riguardo, M.D. Green, M. Freedman, L. Gordis, *Reference guide on epidemiology*, cit., 616, si limitano ad affermare che, se l'attore è in grado di escludere altre note cause della medesima patologia, ad esempio genetiche, aumenta la probabilità che il fattore di rischio abbia causato propria la malattia del danneggiato.

[33] Al riguardo R.R. Weber, *Has the Daubert decision created a new "pest" for California farm workers involved in pesticide poisoning litigation?*, in *San Joaquin Agricultural Law Review*, 2010, 19, 242s., riporta due sentenze d'appello californiane: *Jones v. Ortho Pharm. Corp.*, 209 Cal. Rptr. 467 (Cal. Ct. App. 1985) ha stabilito che «*a possible only becomes a 'probable' when, in the absence of other reasonable causal explanations, it becomes more likely than not the injury was a result of its action*»; analogamente, secondo *Lockheed Litigation Cases*, 23 Cal. Rptr. 3d 762 (Cal. Ct. App. 2005), un rischio relativo inferiore a 2 non esclude necessariamente il nesso causale, se «*expert relies on other factors to show the plaintiff's risk of injury was greater than that of the study subjects or relies on other matters to support the conclusion that causation was more likely than not*». Sull'accertamento del nesso causale nella dottrina statunitense, si rinvia a S.C. Gold, *When Certainty Dissolves into Probability: A Legal Vision of Toxic Causation for the Post-Genomic Era*, in *Washington & Lee Law Review*, 2013, 70, 237; N.C. Stout, P.A. Valberg, *Bayes' Law, sequential uncertainties, and evidence of causation in toxic tort cases*, in *University of Michigan Journal of Law Reform*, 2005, 38, 781; K. Sulyok, *Managing uncertain causation in toxic exposure cases: lesson for the European Court of Human Rights from U.S. toxic tort litigation*, in *Vermont Journal of Environmental Law*, 2017, 18, 519; G.W. Boston, *Toxic apportionment: a causation and risk contribution model*, in *Environmental Law*, 1995, 25, 549; C.H. Johnson, *When science is too daunting: multiple chemical sensitivity, Federal Courts, and the struggling spirit of Daubert*, in *Villanova Environmental Law Journal,* 2000, 11, 273; V.R. Walker, *Restoring the Individual Plaintiff to Tort Law by Rejecting "Junk Logic" About Specific Causation*, in *Alabama Law Review,* 2004, 56, 381; J.R. MacAyeal, *The Comprehensive Environmental Response, Compensation, and Liability Act: The Correct Paradigm of Strict Liability and the Problem of Individual Causation*, in *UCLA Journal of Environmental Law & Policy,* 2001, 18, 217.

causali dell'evento lesivo[34].

Tale affermazione delle Sezioni unite penali non può essere intesa nel senso che sia necessario escludere tutti i decorsi causali alternativi teoricamente possibili. Infatti, il dubbio comporta l'assoluzione dell'imputato solo se ragionevole. Di conseguenza, il pubblico ministero deve escludere non tutti i decorsi causali astrattamente possibili, ma solo quelli di cui c'è motivo di sospettare nel caso concreto; non può motivare l'assoluzione sul fatto che la scienza non ha ancora individuato tutte le cause della malattia del danneggiato[35]. Tale conclusione vale a maggior ragione per la responsabilità civile[36].

La dottrina e la giurisprudenza italiane hanno chiarito che l'indicata procedura di esclusione dei decorsi causali alternativi, da un lato, vale solo nei, pur numerosi, casi di malattie multifattoriali, dall'altro, non è ancora sufficiente a provare la causalità individuale. A tal fine è necessario anche escludere che: *a*) il danneggiato sia stato esposto all'agente patogeno in contesti diversi da quelli di cui deve rispondere il convenuto, ad esempio nell'abitazione del danneggiato o in aziende dove ha lavorato precedentemente, e *b*) il

---

[34] Cass. pen., S.U., 11.09.2001, n. 30328; D. CHINDEMI, *Rischio amianto: elemento soggettivo del reato e nesso di causalità*, in *Resp. civ. prev.*, 2010, 1, 200; D. SANTARPIA, *Dalla Cassazione fumata nera: per il tabagista nessuna salvezza, nemmeno risarcitoria*, in *Resp. civ. prev.*, 2019, 2, 586; G. TRAVAGLINO, *Nessi di causa e prova presuntiva*, in S. PATTI E R. POLI (a cura di), *Il ragionamento presuntivo. Presupposti, struttura, sindacabilità*, Torino, 2022, 274. Secondo Cass. civ., sez. lav., 05.09.2017, n. 20769, consultabile al sito: https://olympus.uniurb.it/index.php?option=com_content&view=article&id=17409:cassazione-civile,-sez-lav-,-05-settembre-2017,-n-20769-carcinoma-dell-operaio-metalmeccanico-addetto-alla-verniciatura-la-causa-della-malattia-%C3%A8-il-tabagismo-o-l-attivit%C3%83%&Itemid=101, «l'ausiliare nominato dal Giudice può giungere al giudizio di ragionevole probabilità anche in base alla compatibilità della malattia non tabellata con la *noxa* professionale, desunta dalla tipologia delle lavorazioni svolte, dalla natura dei macchinari presenti sul luogo di lavoro, della durata della prestazione lavorativa, e per l'assenza di altri fattori extra-professionali, utilizzando, a tale scopo, congiuntamente anche dati epidemiologici, per suffragare una qualificata probabilità». Nello stesso senso già Cass. civ., sez. lav., 10.02.2011, n. 3227, in *Foro it.*, 2011, IV, 1106 ss. Ad integrazione di tale impostazione, Cass. civ., sez. lav., 25.05.2004, n. 10042, ripresa da Trib. Bari, sez. lav. 23.11.2021, n. 3364, consultabile al sito: https://responsabilecivile.it/il-nesso-eziologico-tra-attivita-lavorativa-e-malattia-professionale1/, precisa che «il giudizio di compatibilità si differenzia dalla mera possibilità in quanto il primo implica, oltre l'affermazione che la noxa professionale può avere causato la malattia, anche la esclusione di ogni altro fattore extraprofessionale». Dunque, nei casi in cui il rischio relativo è inferiore a 2 e sussiste una spiegazione causale alternativa, come il fumo di sigaretta, la domanda dovrebbe essere rigettata. In tal senso, App. Genova, sez. lav. 13.04.2018, n. 56, in *De jure*; Trib. Venezia, sez. lav., 19.01.2021, n. 29, in *De jure*: «a fronte di una causa certa di adenocarcinoma – il tabagismo – non soccorrono altre cause certe; come si è detto infatti vi è prova dell'esposizione ma non dell'entità di questa, mentre i criteri di Helsinki richiedono una esposizione qualificata e il rinvenimento di un indicato numero di fibre»; Trib. Taranto, 10.07.2018, n. 1575, in *De jure*: «Quando gli agenti patogeni lavorativi, non dotati di sufficiente efficacia causale, concorrano con fattori extralavorativi dotati, invece, di tale efficacia, è esclusa l'origine professionale della malattia».

[35] S. ZIRULIA, *Esposizione a sostanze tossiche*, cit., 237 ss.

[36] Anche in un caso in cui le conoscenze scientifiche sull'eziologia della malattia (neurinoma del nervo acustico) erano molto scarse e gli unici studi sulla pericolosità dell'esposizione a radiazioni non ionizzanti erano stati condotti su animali, App. Torino, sez. lav., 13.01.2020, consultabile al sito: https://olympus.uniurb.it/index.php?option=com_content&view=article&id=21679:corte-di-appello-di-torino,-sez-lav-,-13-gennaio-2020,-n-904-uso-prolungato-del-cellulare-e-tumore-alla-testa-nesso-causale-secondo-criteri-probabilistici-del-pi%C3%B9-probabile-che-non&catid=72&Itemid=138#:~:text=di%20Torino%2C%20Sez.-,Lav.%2C%2013%20gennaio%202020%2C%20n.,del%20%22pi%C3%B9%20probabile%20che%20non%22, ha riconosciuto il risarcimento sulla base delle seguenti presunzioni: associazione tra tumore raro ed esposizione rara per durata ed intensità alle onde del telefono cellulare; periodo di latenza congruo con i valori relativi a quel tipo di tumore; il fatto che la patologia sia insorta nella parte destra del capo del ricorrente, soggetto destrimane; mancanza di altra plausibile spiegazione della malattia, in realtà dovuta all'insufficienza delle conoscenze eziopatogenetiche.

danneggiato sia stato esposto all'agente patogeno nello stesso contesto lavorativo o abitativo, ma dell'inquinamento devono rispondere soggetti diversi dal convenuto, per la successione di diverse società nella gestione dell'impresa inquinante[37].

Se l'agente patogeno è talmente diffuso da rendere impossibile escludere gli indicati decorsi causali alternativi, può ancora essere provata la responsabilità del convenuto. Ma occorre dimostrare che, senza l'esposizione dovuta al convenuto, l'evento lesivo si sarebbe verificato «in epoca significativamente posteriore o con minore intensità lesiva»[38].

Altro strumento per individualizzare il giudizio causale può essere rappresentato dai marcatori biologici[39]. Ad esempio, la colinesterasi è un enzima necessario per il funzionamento del sistema nervoso sia degli esseri umani sia degli insetti. Gli organofosfati, ampiamente utilizzati come insetticidi in agricoltura, inibiscono la colinesterasi. L'abbassamento dei livelli di colinesterasi, misurabile con l'esame del sangue, può derivare dall'esposizione ad organofosfati e portare a disordini neurologici[40].

I progressi della scienza offrono una nuova e ulteriore prospettiva. Attraverso accertamenti di minima invasività, è possibile verificare se la persona presenta caratteristiche genetiche tali da renderla pienamente capace di detossificare l'impatto della sostanza inquinante con l'organismo oppure, al contrario, maggiormente suscettibile a subire l'effetto lesivo della stessa. La suscettibilità individuale può rivelarsi utilissima ai fini della prova della causalità individuale: anche se, a fronte di analoghe esposizioni alla medesima sostanza

---

[37] S. ZIRULIA, *Esposizione a sostanze tossiche*, cit., 65; M. BARNI, *Il medico legale e il giudizio sulla causalità: il caso del mesotelioma da asbesto*, in *Riv. it. med. leg.*, 2011, 2, 489; M. BONA, *Morti da amianto sul lavoro: il punto su responsabilità e risarcimenti*, in *Resp. civ. prev.*, 2021, 2, 590.

[38] Cass. pen., sez. un., 11.09.2001, n. 30328; Cass. pen., sez. IV, 17.04.2020 n. 12353. Come rileva la citata sentenza Cozzini, per stabilire se l'esposizione dovuta al convenuto abbia contribuito ad anticipare la morte, in concorso con le altre esposizioni che non è stato possibile escludere, «sono necessarie, almeno, informazioni cronologiche, ed occorre poter affermare che il processo patogenetico si è sviluppato in un periodo significativamente più breve rispetto a quello richiesto nei casi in cui all'iniziazione non segua un'ulteriore esposizione»; oppure, in alternativa, «devono essere noti i fattori che nell'esposizione protratta accelerano il processo ed essi devono essere presenti nella concreta vicenda processuale». Nello stesso senso già S. ZIRULIA, *Mesotelioma da amianto e prova della causalità individuale: a volte è possibile*, 13 maggio 2020. Consultabile al sito: https://www.sistemapenale.it/it/scheda/mesotelioma-da-amianto-e-causalita-individuale#_ftnref3. Tale aspetto si pone nel più generale problema delle concause. Normalmente, infatti, le evidenze scientifiche derivano da studi che non sono progettati per indagare il ruolo concausale di un fattore di rischio rispetto ad un altro. In tali ipotesi, difetta un metodo scientifico che consenta di affermare che l'antecedente è condizione necessaria ma non sufficiente dell'evento. Quindi, più che di concausa in senso proprio, si tratta di affermare «che l'attività lavorativa ha caratteristiche biologiche e circostanziali compatibili e convergenti rispetto all'eziologia del danno, muovendo dal riconoscimento di una reale adeguatezza lesiva del lavoro, con il conforto di tempi, sede e modalità di azione, fondata sull'individualità della risposta del singolo, a prescindere dai dati statistici ed epidemiologici, a suffragio della scientificità dell'assunto» (G.A. NORELLI, A. BONELLI, M. FOCARDI, V. PINCHI, *Rigore giuridico ed opportunità sociale nella valutazione della "concausa" di malattia professionale*, in *Riv. it. med. leg.*, 2015, 3, 894 s.s., in particolare 897 s.)

[39] S. ZIRULIA, *Esposizione a sostanze tossiche*, cit., 13.

[40] S.Y. GANIE, D. JAVAID, Y.A. HAJAM, M.S. RESHI, *Mechanisms and treatment strategies of organophosphate pesticide induced neurotoxicity in humans: A critical appraisal*, in *Toxicology*, 2022, 472, 1-10; M. AMIN, M. YOUSUF, M. ATTAULLAH, N. AHMAD, M.N. AZRA, M. LATEEF, I.D. BUNERI, I. ZEKKER, G. EL-SABER BATIHA, S.M. ABOELENIN, M. ZAHOOR, M. IKRAM, M. NAEEM, *Cholinesterase activity as a potential biomarker for neurotoxicity induced by pesticides* in vivo *exposed Oreochromis niloticus (Nile tilapia): assessment tool for organophosphates and synthetic pyrethroids*, in *Environ. Technol.*, 2022, 1-9; R.R. WEBER, *Has the Daubert decision created a new "pest" for California farm workers involved in pesticide poisoning litigation?*, cit., 244ss.

inquinante, solo alcuni si ammalano, nel caso dell'attore proprio quella sostanza ha avuto un ruolo concausale perché egli è meno capace di detossificarne l'effetto lesivo. In altri termini, la suscettibilità individuale del danneggiato si pone quale concausa naturale della malattia, ma quest'ultima non si sarebbe verificata (o sarebbe insorta in epoca significativamente posteriore) senza l'esposizione all'agente patogeno[41]. Quindi, gli accertamenti medici di suscettibilità individuale sembrano porsi come passaggio fondamentale di qualunque elaborato peritale.

Il fatto che la suscettibilità individuale si ponga come concausa naturale preesistente pone il problema dei suoi effetti sulla responsabilità. La giurisprudenza tradizionale era solita escludere qualsiasi rilevanza della concausa naturale in ragione del criterio condizionalistico e del principio di equivalenza delle cause, sanciti dagli artt. 40 e 41 c.p. e ormai da tempo pacificamente applicati alla responsabilità civile[42]. Più di recente, la Suprema Corte ha sostenuto che la concausa naturale riduca di per sé la responsabilità del danneggiante in virtù dell'applicazione analogica dell'art. 1227 c.c. [43]. Tuttavia, l'attuale orientamento ha chiarito che la concausa naturale può comportare una diminuzione del risarcimento ex art. 1223 c.c. solo nei casi e nella misura in cui, eliminandola mentalmente, il danno conseguenza risulti di minore entità (c.d. menomazione concorrente)[44]. Infatti, in tale ipotesi, il danno complessivo non è interamente (con)causato in via immediata e diretta dal fatto illecito: quest'ultimo colpisce la preesistente menomazione, aggravandone l'effetto pregiudizievole sull'integrità psico-fisica. Di conseguenza, una parte di questo pregiudizio complessivo è prodotta indirettamente dal fatto illecito. Quindi il risarcimento deve essere ridotto. Nelle altre ipotesi, ossia quando la preesistenza naturale, ad esempio la pregressa patologia, concausa l'evento lesivo oppure concausa la menomazione (ossia il danno conseguenza), ma, eliminando mentalmente la preesistenza, il danno conseguenza risulti invariato (c.d. menomazione

---

[41] L.M. Dong, J.D. Potter, E. White, C.M. Ulrich, L.R. Cardon, U. Peters, *Genetic Susceptibility to Cancer: the Role of Polymorphisms in Candidate Genes*, in *Journal of the American Medical Association*, 2008, 20, 2423; C. Dieter, L. de Almeida Brondani, C. Bauermann Leitão, F. Gerchman, N. Emerim Lemos, D. Crispim, *Genetic polymorphisms associated with susceptibility to COVID-19 disease and severity: A systematic review and meta-analysis*, in *Plos One*, 6 luglio 2022. Consultabile al sito: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0270627; Y. Wang, R. Wang, S. Yuan, X. Liu, *Genetic polymorphisms of CYP24A1 gene and cancer susceptibility: a meta-analysis including 40640 subjects*, in *World Journal of Surgical Oncology*, 2023, 21, 279.

[42] Cass. civ., sez. III, 09.04.2003, n. 5539; Cass. civ., sez. III, 16.02.2001, n. 2335, in *De jure*; C.M. Bianca, *Diritto civile*, V, *Responsabilità civile*, Milano, 2012, 142 ss.

[43] Cass. civ., sez. III, 16.01.2009, n. 975, in *Resp. civ. prev.*, 2010, 2, 375, con nota di G. Miotto, *Il "difficile" concorso di cause naturali e cause umane del danno*; L. Nocco, *Dalla perdita di* chance *alla responsabilità proporzionale: ovvero come ripartire i rischi in sanità*, in *Riv. it. med. leg.*, 2014, 4, 1209; B. Guidi, *Il modello della causalità proporzionale e la rilevanza dei fattori naturali: l'applicazione al contenzioso da patologia amianto-correlata*, in *Riv. it. med. leg.*, 2012, 4, 1577; F. Della Negra, *La Suprema Corte ritorna sulla questione delle concause naturali: una terza via?*, in *Riv. it. med. leg.*, 2012, 4, 1772; D.M. Frenda, *«Multifattorialità dell'evento» e perdita di* chances *nella responsabilità medica: risarcimento parxziale, risarcimento proporzionale, risarcimento equitativo … nessun risarcimento?*, in *Resp. civ. prev.*, 2021, 2, 379; R. Pucella, *Il perimetro dell'accertamento causale tra colpa, concause e danno risarcibile*, in *Resp. civ. prev.*, 2016, 4, 1111.

[44] Cass. civ., sez. III, 11.11.2019, n. 28986, in *Resp. civ. prev.*, 2020, 3, 808, con nota di M. Bona, *Il calcolo del 'danno differenziale' da invalidità preesistente: questione risolta dalla 'doppia valutazione' di 'San Martino 2019'?*; P. Libeccio, *Sulla rilevanza della concausa naturale nella responsabilità extracontrattuale*, in *Resp. Civ. prev.*, 2021, 2, 656; N. Rizzo, *Il problema delle concause dell'evento dannoso nella costruzione del modello civile di causalità giuridica: introduzione a una teoria*, in *Resp. civ. prev.*, 2022, 3, 713.

coesistente), gli artt. 40-41 c.p. e 1223 c.c. comportano la responsabilità risarcitoria per tutti i pregiudizi ingiusti subiti dal danneggiato perché nessuno di essi si sarebbe verificato senza la condotta illecita e tutti ne derivano in via immediata e diretta[45].

4. Conclusioni.

Il problema della causalità continua a porsi come difficilmente sormontabile per gli attori nel contenzioso da inquinamento ambientale.

Tuttavia, l'evoluzione della giurisprudenza civile e delle conoscenze medico-legali ed epidemiologiche concorrono a rendere prevedibile un aumento delle possibilità di dimostrare il nesso causale. Il criterio della *preponderance of the evidence*, la ridotta rilevanza delle concause naturali, l'individuazione di una metodologia attendibile e concretamente applicabile nell'accertamento della causalità generale e l'irrilevanza dei decorsi causali alternativi meramente ipotetici sono dati che rendono più accessibile per i danneggiati la prova del nesso causale.

A tal fine appare necessario che i giudici stimolino i loro consulenti alla ricerca di evidenze scientifiche elaborate conformemente alla metodologia accreditata e sulla base di coorti di partecipanti il più possibile simili al danneggiato. Un ruolo importante riveste anche la cooperazione tra difensore e consulente delle singole parti, specie nella verifica del passaggio dalla causalità generale a quella individuale.

[45] Cass. civ., sez. III, 23.02.2023, n. 5632, in *De jure*, la quale precisa che «qualora resti comunque incerta la misura dell'apporto concausale naturale, la responsabilità di tutte le conseguenze individuate in base alla causalità giuridica va interamente imputata all'autore della condotta umana». Già la tradizionale dottrina medico-legale aveva distinto tra concause naturali di lesione, che non riducono il risarcimento perché tutti danni conseguenti all'evento lesivo sono concausati dal fatto illecito, e concause naturali di menomazioni concorrenti, che invece depauperano il risarcimento perché non tutto il danno-conseguenza si sarebbe verificato senza l'interazione di tale concausa (C. GERIN, *La valutazione medico-legale del danno alla persona in responsabilità civile*, Milano, 1987; G. MONTANARI VERGALLO, N.M. DI LUCA. P. FRATI, *Chances perdute e rispettiva rilevanza della colpa e delle cause naturali nell'accertamento della causalità civile medica: dalla probabilità prevalente all'equità*, in *Riv. it. med. leg.*, 2011, 1, 61; A. FIORI, D. MARCHETTI, G. LA MONACA, *La causalità civile ed i suoi perduranti problemi medico-legali*, in *Riv. it. med. leg.*, 2014, 3, 1073).

Coppola I, Cordoba LI, Móron AS, 'Qualche considerazione critica sull'eredità digitale, *tra patrimonio e dati* un complicato bilanciamento di interessi nella tematica testamentaria' (2023) 2 EJPLT, 169 - 186.
DOI: https://doi.org/10.57230/EJPLT232ICLICASM

EJPLT
ISSN 2704-8012

Qualche considerazione critica sull'eredità digitale, *tra patrimonio e dati* un complicato bilanciamento di interessi nella tematica testamentaria

Some critical considerations on digital inheritance, between assets and data a complicated balancing of interests in testamentary matters

LUCILA INÉS CÓRDOBA
Professore Associato in Diritto di famiglia e successioni
Università di Buenos Aires

ADRIANA SYLVINA MÓRON
Ricercatore di Diritto privato
Università Abierta Interamericana

IRENE COPPOLA
Assegnista di ricerca in Diritto privato
Università degli Studi di Napoli Federico II

Abstract

L'obiettivo di questo lavoro è quello di evidenziare la necessità che la cosiddetta eredità digitale non solo venga identificata concettualmente al netto di speculazioni astratte, ma che abbia anche una regolamentazione normativa ad hoc, atteso che appare essere complicato una definizione omnia per far posto piuttosto ad una distinzione tra i tradizionali beni fisici e quelli innovativi di registro digitale costituenti patrimonio restante del de cuius. Il tema in argomento necessita di un rafforzamento della cultura testamentaria e di un nuovo smalto per la figura dell'esecutore.

The objective of this paper is to highlight the need for the so-called digital inheritance not only to be identified conceptually net of abstract speculation, but also to have ad hoc normative regulation, since it appears to be complicated to have an omnia definition to make way rather for a distinction between traditional physical assets and innovative digital registry assets constituting the remaining assets of the de cuius. The topic at hand needs a strengthening of testamentary culture and a new polish for the figure of the executor.

© The author(s) 2023, 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: eredità digitale; dato digitale e dato fisico; regolamentazione *ad hoc.*

Summary: 1. Breve introduzione. – 2. La ricostruzione digitale della vita contro l'idea della morte. Il ricordo digitale corporeo è un'eredità? – 3. L'eredità digitale come declinazione del concetto di eredità o come nuova categoria di innovazione consapevole? Dal dato al bene: dal digitale al fisico. – 4. Pianificazione successoria e*governance* delle piattaforme. – 5. Profili commemorativi nelle piattaforme. Giurisprudenza tedesca, giurisprudenza americana. – 6. Qualche conclusione.

1. Breve introduzione.*

La società postmoderna immersa nell'era digitale è stata chiamata società dei consumi[1]; Zygmunt Bauman. Brzezinski la definisce tecnotronica[2] e lo spagnolo Manuel Castells la inquadra come società in rete.[3] La stessa configurazione di ByungChul Han, filosofo sudcoreano, di società della trasparenza – caratterizzata dall'esposizione della vita su reti sotto un panopticon digitale – evoca l'opera di Orwell del 1984 in cui la vita degli individui era controllata dallo schermo del Grande Fratello[4] ed in questo evidente sciame digitale[5] emerge che la tradizionale tripartizione dei poteri del Montesquieu appare avere oggi un sapore anacronistico di fronte al nuovo ed incontrollato potere digitale[6].

Stefano Rodotà afferma che <<si avvicina quello che un gruppo di ricercatori dell'Unione Europea ha descritto come uno tsunami digitale, che può stravolgere gli strumenti giuridici che garantiscono l'identità e perfino la libertà delle persone. Una trasformazione radicale delle nostre organizzazioni sociali è tra noi>>[7]. È così che i sistemi di intelligenza artificiale che utilizzano tecnologie dirompenti sono già una evidente realtà nel nostro ordinamento giuridico.[8]

---

* Irene Coppola è autore dei paragrafi: 2, 3, 4, 6; Lucila I. Cordoba e Adrana Moron sono le autrici dei paragrafi: 1,5,6.

[1] Z. Bauman, *Vida de Consumo*, *Fondo de Cultura Económica*, Buenos Aires, 2008 y *Mundo Consumo,* Paidós, Buenos Aires, 2010, *passim.*

[2] A. Alterini, *El consumidor en la sociedad posmoderna*, LA LEY 1996-E, 818; RCyS 2017-X , 283; Cita: TR LALEY AR/DOC/10407/2001

[3] A. Andruet, *Libertad de expresión de los jueces en las redes sociales: sociabilidad y conectividad*, Publicado en: SJA 26/08/2022, 1; JA 2022-III, 131; TR LALEY AR/DOC/2401/2022.

[4] B. Chul Han, *La sociedad de la transparencia,* Herder, Barcelona, 2013, 11.

[5] En su obra *En el enjambre* (Herder, 2014, 11 el filósofo surcoreano Byung-Chul Han expresa que nos embriagamos hoy con el medio digital, sin que podamos valorar por completo las consecuencias de esa embriaguez.

[6] A. Maniaci, *Eredità digitale: cos'è e come si può trasmettere*, Altalex del 18 giugno 2020.

[7] S. Rodotà, *El derecho a tener derechos*, Ed. Trotta, Madrid, 2014, 298, citado por ADARO, Mario, "La formación de las abogadas y los abogados ante la digitalización del proceso", LA LEY 31/08/2020, 4, LLOnline: AR/DOC/2881/2020.

[8] M. Adaro spiega che in ambito giuridico sono emerse esperienze con software automatizzati per la redazione di atti giudiziari, contratti intelligenti (smart contracts), avvocati androidi o cyborg (robot avvocato Ross), algoritmi per la risoluzione delle controversie legali e per la previsione di sentenze (Watson-IBM), l'uso dell'intelligenza artificiale per i sistemi giudiziari (caso Prometea, un sistema

Né appare eccessivo, in questo contesto, il pensiero di Anand Rao, secondo cui all'inizio del XXI secolo, l'evoluzione tecnologica e la convergenza di molteplici fattori hanno aiutato l'Intelligenza Artificiale "a passare dall'ambiente in vitro (laboratori di ricerca) all'ambiente in vivo (la vita quotidiana)"[9].

Consegue che appare non tanto straordinario (nell'accezione di *extra-ordinem*) che proprio il diritto successorio, da tempo monolite degli ordinamenti ed in particolare dell'ordinamento italiano, quasi santone intoccabile sulle alte vette dell'Himalaya – con qualche ingessatura granitica consolidata negli anni – possa diventare oggetto di dibattito da parte della ricerca in quanto attinto con tanto interesse dalla rivoluzione copernicana del digitale che tutti noi stiamo vivendo in una nuova pratica che appare essere struttura sovrapposta e sovrapponibile ai vecchi archetipi di impostazione della compagine sociale.

Ed in questo contesto ci si apre alla innovazione, anche se non va trascurato che occorre verificare che tipo di innovazione sia compatibile con il sistema giuridico attuale, soprattutto quando va a delinearsi l'espressione ellittica o brachilogica di eredità digitale, pur sempre e comunque nel rispetto del diritto successorio nella sostanza fondato, come è noto, sul riconoscimento della proprietà privata e dei rapporti familiari.



2. La ricostruzione digitale della vita contro l'idea della morte. Il ricordo digitale corporeo è un'eredità?

Il Codice Civile italiano risalente ad un'epoca calata in un segmento sociale diverso – con la deriva di un concetto di proprietà fortemente intesa come proprietà fondiaria caratterizzata da una declinazione soprattutto fisica del bene – non contempla (come ovvio) nessun riferimento al digitale, al bene digitale ed all'eredità digitale, ma non contiene nemmeno alcuna regola interdittiva.

---

intelligente che ha avuto i suoi esordi nell'agosto 2017 presso la Procura Generale Aggiunta per il Contenzioso Amministrativo e Fiscale della Procura della Città di Buenos Aires) e/o giudici robot (l'Estonia, nel 2019, è già nella prima fase di test pilota del progetto giudici robot, ovvero l'implementazione dell'intelligenza artificiale per le decisioni giurisdizionali). ADARO, Mario, "La formación de las abogadas y los abogados ante la digitalización del proceso", LA LEY 31/08/2020, 4, LLOnline: AR/DOC/2881/2020.

[9]AS. RAO, *Una nueva etapa de la globalización*, publicado en AA.VV., *Algoritmolandia. Inteligencia Artificial para una integración predictiva e inclusiva de América Latina*, Integración & Comercio # 44, Julio 2018, Ed. Planeta, Buenos Aires 2018, 1ª ed., 51-52, citado por SUEIRO, Carlos, Christian, "Inteligencia artificial y vigilancia electrónica", Publicado en: DPyC 2020 (noviembre), 69; TR LALEY AR/DOC/3325/2020



Ricostruzione digitale della ragazza coreana morta

Ora, se l'eredità va intesa, secondo il diritto positivo, come l'insieme di tutti quei diritti e di obblighi del defunto che non si estinguono con la sua morte, occorre indagare sul dato o sul bene digitale e sulla trasmissibilità del relativo diritto nel *post mortem*.

Lo stesso tema della morte (e, quindi, della finitezza della vita) attualmente viene discusso e trattato in modo diverso registrandosi anche casi di ricostruzione, per mezzo di raffinatissime tecniche di intelligenza artificiale, della stessa immagine corporea del defunto al fine di perpetrarne il ricordo in una realtà virtuale, come è accaduto nella Corea del Sud dove, per consentire alla non rassegnata madre di riavvicinarsi e di incontrare ancora la compianta figlia, si è provveduto a creare attraverso la realtà virtuale il corpo e la mente della ragazza con apposito dispositivo di intelligenza artificiale appositamente addestrato; difatti il documentario Meeting You, trasmesso dalla rete televisiva coreana MBC, mostra il ricongiungimento della madre con la figlia di sette anni (morta a causa della malattia HLH da disturbo di immunodeficienza). In altri termini, la ragazza morta rivive in una densità corporea artificialmente creata e dialoga virtualmente con la madre attraverso una sistema A.I. istruito sulla base di interviste con membri della famiglia e dati video[10].

L'idea di far tornare in vita i propri cari defunti utilizzando la realtà virtuale appare essere risalente, atteso che nel 2015 Paranormal Games ha annunciato Project Elysium, un sistema il cui obiettivo è un'esperienza VR personalizzata dell'aldilà che riunisce le persone con i loro cari morti.

[10] https://www.xataka.com/realidad-virtual-aumentada/recrean-a-nina-siete-anos-fallecida-su-madre-pueda-reunirse-ella-usando-realidad-virtual, página compulsada el 20/1/2023.



Ancor più di recente in America si registra la presenza del defunto ai propri funerali attraverso la ricostruzione corporea del morto realizzata con una intelligenza artificiale[11].

Si è di fronte a nuove tipologie contrattuali consapevoli di realtà alternative a quella concreta e reale.

In queste ipotesi la creazione virtuale di persone decedute implica, da parte degli eredi e della società, la stipula di un contratto che si potrebbe definire di umanizzazione; se vi è accordo nulla *quaestio* anche se bisognerebbe in ogni caso chiedersi se trattasi di contratti lesivi della dignità umana.

Il dibattito resta aperto e l'oggetto va esteso non solo sul contenuto del cosiddetto di contratto di umanizzazione, ma anche sul dubbio circa la possibilità o meno di configurare nel concetto di eredità la ricostruzione corporea di una persona deceduta.

Il tema è delicato e non di facile soluzione tanto è vero che vi è già qualche precedente contenzioso in tale ambito: difatti, nell'anno 2012 si registra un contrasto tra la società titolare dei diritti di immagine di Marilyn Monroe e una start-up titolare del brevetto VM2 - The Virtual Marilyn, la prima attrice virtuale vivente; la stessa società, però, dopo i primi passi verso un contenzioso giudiziario, preferisce lascia perdere e abbandona il progetto di ricostruzione virtuale della diva[12].

Sta di fatto che l'accelerazione della rivoluzione tecnologica è una realtà innegabile anche nel momento dominato dalla morte con conseguenti sfide ed interrogativi complessi.

Indubbiamente nel nuovo approccio digitale il concetto della memoria del defunto si amplia; i suoi blog, i suoi profili *social*, il suo *nickname* nelle comunità virtuali, l'avatar, la mail, le password, le credenziali di accesso, le arti figurative digitali, etc. integrano una parte importante della vita digitale del defunto: una identità digitale la cui traccia trova cittadinanza nella resistenza tecnologica dando luogo ad una sorta di estensione digitalmente valutabile.[13]

Ma anche l'identità corporea in versione *digita*l, ovvero il ricordo dell'aspetto fisico, dell'immagine personale (che non sia una semplice foto) o della voce del defunto costituiscono beni nella disponibilità degli eredi?

La questione è molto complessa ed allo stato sembrerebbe doverosa una

---

[11] Rai, Radio Televisione Italiana TG del 21 gennaio 2024.

[12] https://www.innovaciondigital360.com/i-a/hologramas-3d-para-revivir-a-las-estrellas-del-pasado/, página compulsada el 21/1/2023.

[13] A. GIL DOMINGUEZ, *El fallo "CFK": La Corte Suprema como poder del estado y la democracia digital*, Publicado en: LA LEY 28/05/2020, 13; Cita: TR LALEY AR/DOC/1517/2020.

risposta negativa, atteso che l'identità del defunto e la sua fisicità fatta rivivere in un mondo virtuale non risultano essere trasmissibili agli eredi secondo l'attuale archetipo normativo.

Certo una rivisitazione dell'assetto normativo dovrebbe essere oggetto di un intervento da parte di un legislatore consapevole e responsabile.

3. L'eredità digitale come declinazione dell'eredità o come nuova categoria di innovazione consapevole. Dal dato al bene tra *digitale e fisico*.

Nell'ottica non definitoria del codice civile italiano non vi è alcuna esplicazione di eredità se non nei richiami della categoria in astratto, sempre non definitori, di cui, a titolo esemplificativo, agli articoli 457, 459, 470-483, 484, 528-532, 519-527, 1542-1547 c.c.

Se per eredità va inteso, ormai in modo pacifico, l'insieme dei diritti e degli obblighi trasmissibili dal defunto a terzi (eredi o legatari) nel *post mortem*, allora consegue che, nell'espressione contemporanea ed ellittica di eredità digitale, vada incluso tutto ciò che, pur avendo natura digitale, possa essere oggetto di diritto trasmissibile ad eredi o legatari.[14]

In altre parole, per eredità digitale occorre intendere appieno il concetto sostanziale di patrimonio digitale *trasmissibile mortis causa* ed il punto è proprio questo: quali sono i dati digitali che diventano beni ed in quanto tali trasmissibili o, più precisamente, quali sono i diritti digitali trasmissibili?

Il diritto digitale trasmissibile nel *post mortem* o *mortis causa* – come principio generale riconducibile al diritto privato – va sottratto al concetto di indisponibilità come accade per i diritti della personalità o dei diritti personalissimi. Il problema diventa più complesso quando occorre individuare in positivo dati o beni digitali collegati ad un diritto, indisponibile o disponibile, del defunto.

Procediamo, con una breve analisi, per gradi: quando un bene può definirsi

[14] Il primo tribunale italiano a declinare l'espressione eredità digitale è stato quello di Milano con sentenza del 10/2/2021 in relazione ad opere d'arte digitali facenti capo ad un artista deceduto. L'ordinanza cautelare del Tribunale di Milano si sofferma in un'analisi più della normativa relativa al trattamento di dati personali che della disciplina delle successioni, ha riconosciuto ai dati facenti capo al defunto e custoditi all'interno di un account allo stesso riconducibile la natura di beni oggetto di devoluzione mortis causa. Il commento coglie l'occasione soprattutto per mettere in luce le principali criticità connesse alla tutela dei dati personali *post mortem* e, più in generale, al fenomeno della successione in rapporti digitali, Cfr. A. MANIACI, *La prima decisione italiana in tema di "eredità digitale": quale tutela post mortem dei dati personali?* in *Il Corriere Giuridico*, n. 5, 2021, 661 e ss.; C. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf.*, 2018, 65 ss., la quale evidenzia la complessità del fenomeno rilevando che, da una parte, "il termine 'eredità' sul piano tecnico giuridico fa riferimento ad un processo di circolazione dei diritti, e dei beni che ne sono oggetto, quali componenti di un patrimonio che - in atto o in potenza - è suscettibile di valutazione economica e che comunque attiene primariamente alle dinamiche di attribuzione della ricchezza materiale e alla garanzia della continuità del potere di disporre della stessa nell'ambito di una famiglia; ma anche alla garanzia della continuità dei rapporti economici indipendentemente dalla morte dei soggetti che ne sono parti" e, dall'altra, "l'aggettivo 'digitale' stravolge o modifica sensibilmente questo scenario.

digitale[15]?

Qualche autore afferma che <<il bene digitale è caratterizzato dall'essere di natura immateriale, incorporea, che è archiviato, registrato o conservato in supporti elettronici o digitali virtuali, sia localmente (il proprio computer, disco rigido esterno, ecc.) sia su server cloud, nel cloud (Dropbox, iCloud), o in modalità mista, mantenendo l'intero file localmente e il suo riepilogo o hash nel cloud>>[16]; l'ampiezza dell'idea di bene digitale sta nel fatto che esso costituisce anche l'impronta digitale di una persona e che consente la costruzione della sua identità e della sua attività digitale[17].

Altri sostiene che con la morte di un soggetto i suoi blog, i suoi profili nelle reti sociali, i suoi pseudonimi nelle comunità virtuali comincino a integrare la memoria della morte come *post mortem* di identità digitale[18]; il concetto di memoria defunta presuppone, ergo, un'estensione della personalità che suscita quella meritevolezza tutelabile, anche se trattasi di entità *on line* e non fisicamente palpabile, alla stregua di qualsivoglia diritto anche della personalità, quali immagine e *privacy*.

Interessante appare la distinzione tra beni digitali patrimoniali e beni digitali non patrimoniali; i primi inquadrabili come beni giuridici e, pertanto, con caratteristiche di commerciabilità, negoziabilità e trasmissibilità; i secondi come beni immateriali, estranei al commercio, con valore talvolta sentimentale o personale quali mail, video, immagini, foto, etc.; Flores spiega che questi beni, in linea di principio, sarebbero fuori dal trasferimento successorio, e quindi non protetti dal diritto di proprietà, ma da altri diritti come la privacy, l'onore e l'immagine che si estinguono con la morte del titolare, fatta sempre salva la tutela *post mortem* per la privacy, l'immagine e

---

[15]A. MANIACI, A. d'ARMINO MONFORTE, *L'eredità digitale tra silenzio della legge ed esigenze di pianificazione negoziale,Il Corriere Giuridico*, n.11, 2020, 1367 e ss.; A. MANIACI, *Eredità digitale e accesso ai dati personali del defunto*, in *Diritto di Internet*, n. 3, 2022, p.561-567: Tribunale di Roma; sezione ottava; ordinanza 10 febbraio 2022: è ammissibile e fondata la domanda cautelare ex art. 700 c.p.c. volta ad ottenere in via d'urgenza l'ordine di fornire assistenza nel recupero dei dati personali dagli account del coniuge deceduto, attesa la legittimazione iure proprio del coniuge superstite, sulla base di un interesse meritevole di protezione di natura familiare, ad esercitare la prerogativa prevista dall'art. 2-terdecies, 1° comma, D.Lgs. n. 196/2003, in combinato disposto con l'art. 15 del Regolamento n. 679/2016, consistente nel diritto di acquisire i dati personali riferibili al defunto, quali foto e filmati di famiglia (integrante gli estremi del c.d. *fumus boni iuris*), e considerata la circostanza per cui il mancato utilizzo di un account i-cloud per un periodo prolungato comporterebbe l'automatica distruzione dei dati ad esso associati (integrante gli estremi del c.d. *periculum in mora*).

[16]N.LAMBER, D. NÉSTOR, *Los bienes digitales en la herencia*, DFyP 2019 (junio), 91. La Ley Online: AR/DOC/1495/2019.

[17] Problematica particolarmente sentita anche nell'ambito delle criptovalute (ovvero di quelle monete virtuali prive di un controvalore garantito da un soggetto terzo e accessibili attraverso una chiave crittografica, destinate all'investimento, alla detenzione o all'uso esattamente come la moneta avente corso legale, con la differenza che le transazioni possono essere realizzate solo attraverso strumenti tecnologici, ossia attraverso la *blockchain*) in quanto al variare della loro forma di detenzione, può mutare anche la possibilità di ottenerne effettivamente il possesso. Il patrimonio ereditario digitale può dunque dirsi composto da beni immateriali eterogenei che necessitano (anch'essi) di essere trasmessi mortis causa nonostante le criticità legate alla presenza di chiavi di accesso (note solo al loro creatore) e l'assenza di strumenti giuridici dedicati alla successione digitale.

[18]J.GONZALES GRANADO, JAVIER , *Solo se muere una vez: ¿Herencia Digital?, in Testamento Digital* coordinado por O. Leon, R. Valero Bancelò, Sonsoles, 2016, España,41, chrome-extension://ieepebpjnkhaiioojkepfniodjmjjihl/data/pdf.js/web/viewer.html?file=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Flibro%2F657167.pdf, página consultata el 3/12/2022.

l'onore[19].

Entrando ancor più in *medias res* , probabilmente non avrebbe molto senso distinguere il bene, in ragione del supporto che lo contiene, in digitale o fisico, per la evidente ragione che si negherebbe ogni differenza proprio perché il supporto (ad esempio il calcolatore come contenitore) è pur sempre dotato di corporeità e quindi di fisicità e non ci sarebbe mai l'evidenza del formato digitale della *res*; né può tacersi che il bene digitale viene, per lo più, racchiuso in un supporto o dispositivo dotato di corporeità, quali il calcolatore, la *pen drive*, lo *smartphone*, gli *hard disk*, i *cd*, i *dvd* etc. cioè qualsiasi supporto su cui vengono archiviate le informazioni, senza escludere risorse digitali tra messaggi e-mail privati, opinioni, stati, fotografie, video, etc.

Ed allora forse sarebbe più corretto operare un'altra distinzione: 1) i beni digitali che si trovano su supporti analogici o fisici di proprietà del defunto; 2) beni digitali che si trovano in un server o sistema digitale di proprietà di un terzo, collegato al defunto attraverso un contratto di consumo.

Nel primo caso (cellulari, tablet etc. etc.) – anche sfruttando il principio dell'accessione – il bene si trova tra i beni personali di proprietà del defunto ed è trasmissibile secondo la regola generale del diritto successorio. A corroborare questa impostazione Merle Bock afferma che "per i dati digitali che sono conservati nelle cose fisiche, la proprietà sulla cosa consente l'accesso a quei dati e quindi segue il destino della cosa a cui è incorporato e trasmesso nella sua custodia agli eredi."[20]

La soluzione diventa più complessa nella seconda ipotesi, ossia quando i beni digitali si trovino su *server* o sistemi digitali, che sono di proprietà di terzi e sono oggetto di un contratto con il consumatore - *is de cuuis hereditate agitur*, concluso in modalità *on.line*, come per l'account.[21]

Innegabile è che per quanto riguarda i server di telecomunicazioni, come e-mail, Facebook, Instagram, Twitter, TikTok, ci troviamo di fronte a pretese di eredi del defunto che potrebbero implicare violazioni di diritti alla privacy, all'intimità[22].

---

[19] M. A. FLORES, *Herenciadigital: un nuevodesafío para elderechosucesorio*, DFyP 2020 (junio), 17/06/2020, 143, LLonline: AR/DOC/3253/2019; I. MASPES, *Successione digitale, trasmissione dell'account e condizioni generali di contratto predisposte dagli internet services providers,*in *I Contratti*, n. 5 2020, 583-590*;* si evidenzia l'intricato rapporto tra diritto all'accesso e tutela della privacy, richiamando l'attenzione sulle condizioni generali di contratto imposte dai fornitori di servizi online. Quest'ultime, infatti, implicano una cessione dei dati personali, sollevando interrogativi sul bilanciamento tra il diritto di accedere ai servizi digitali e la necessità di proteggere la sfera privata degli utenti.

[20]M. BOCK, *JuristischeImplikationendesdigitalenNachlasses*, in Archivfür die civilistische Praxis, 3, vol. 217, Alemania, 2017, 380, citado por M. A, FLORES, Martín Andrés "Herenciadigital: un nuevodesafío para elderechosucesorio", DFyP 2020 (junio), 17/06/2020, 143, LLonline: AR/DOC/3253/2019.

[21]J. C. Faliero., *Los desafíos jurídicos del big data. Tensiones de derechos entre la parametrización analítica, la toma automatizada de decisiones, el targetting y el perfilamiento*, Sup. Esp. LegalTech II 2019 (nov.), 71. Per una definizione di account si v. V. BARBA, *Contenuto del testamento e atti di ultima volontà, Napoli, 2018,* 284: "l'insieme di funzionalità, strumenti e contenuti, che vengono attribuiti a un singolo utente, al quale vengono fornite delle credenziali (nome utente e *password*) per accedervi. L'*account* descrive, dunque, il luogo virtuale privato, nel quale ciascun utente ha un proprio spazio per la conservazione dei propri *files* e nel quale può compiere quelle attività connesse al servizio, di volta in volta offerto dal singolo *provider*"; A. VESTO, *Successione digitale e circolazione dei beni* online. *Note in tema di eredità digitale*, Napoli, 2020, *passim*.

[22] Il D.Lgs. 10 agosto 2018, n. 101, nell'adeguare la normativa nazionale in materia di *privacy* alle disposizioni del Reg. UE 2016/679, ha previsto una disciplina specifica per il trattamento dei dati personali delle persone decedute. Sul tema, P. PATTI - F. BARTOLINI, *Digital Inheritance and post mortem data*

Né sembra corretto tecnicamente affermare, in astratto, un diritto ereditario senza conoscere i termini del contratto che ha legato il consumatore alla piattaforma; difatti, nulla esclude che all'interno del negozio possa essere stata discussa e quindi negoziata l'evenienza del decesso e di cosa sarebbe successo *post;* quello che va discusso e studiato, però, certamente meritevole di tutela, è l'accesso al contratto del defunto per vagliarne il contenuto e la trasmissibilità nel *post mortem*.

La soluzione ed il distinguo in termini pratici non è sempre semplicissima, ed allora sembrerebbe più corretto, allo stato dell'arte, valutare caso per caso[23] e non addivenire a generalizzazioni pericolose per la tutela dei diritti meritevoli.

4. L'esecutore testamentario nella pianificazione successoria digitale e nella *governance* delle piattaforme.

L'attuale approccio digitale sempre più crescente favorisce l'attenzione su quella che, secondo terminologia mutuata dal diritto comparato, viene definita <<pianificazione successoria>>, soprattutto quando si registra una vera complessità nel cercare o ricercare tutti i dati digitali del defunto; di qui si tende a pianificare, a programmare e a predisporre una sorta di << riparto>> successorio per mezzo della stesura di un testamento (al fine di evitare i rischi di una successione *ab intestato*) con la nomina non di un curatore (fallimentare) quanto piuttosto di un esecutore testamentario a cui dare strumenti (chiavi di accesso, nomi utente, password per accedere agli account e/o ai social network) ed istruzioni dettagliate sulla futura amministrazione del patrimonio digitale [24].

Un vero e proprio piano di riparto a favore di chiamati con la necessità che il defunto indichi all'esecutore testamentario oltre alle modalità di accesso su piattaforme, anche disposizioni in ordine al desiderio o meno che tra i suoi account o le sue fotografie o le sue opere d'arte digitali venga cancellato qualche elemento.

Questo nuovo scenario finisce con il condurre ad una riflessione circa il bisogno di una cultura testamentaria che valga non solo a rendere autentica la volontà del testatore, attraverso una specifica formazione, ma che serva anche a disporre su beni di natura digitale che non sempre possono essere catalogati come commerciabili o personali sottraendoli a qualsiasi censura di

---

protection, cit., 1181 ss., I quali, da un confronto fra la disciplina vigente nell'ordinamento tedesco e quello italiano, rilevano come "the BGH stated that the heirs' right to access the Facebook *account* of the deceased follows directly from the principle of universal succession (which is also paramount under Italian law). Such a principle played a pivotal role in the construction of the BGH's reasoning in the absence of specific legislative rules. The Italian legal system shows a different framework in which data protection rules are at the forefront. In this context, Legislative Decree no. 101 of 2018 includes in the list of persons entitled to exercise the GDPR rights of the deceased a person whom the deceased has appointed to protect her interests as an ag.

[23] Sul tema, G. RESTA, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in *Contr. e impr.*, 2019, 86.

[24] G. RESTA, *La successione nei rapporti digitali* e la tutela post-mortale dei dati personali, in *Contr. e impr.*, 2019,86 riporta che secondo alcune stime "circa 10.000 titolari di *account* Facebook muoiono ogni giorno; 312.000 ogni mese; il 5% degli *account* esistenti attengono a 'zombie' digitali"; Id., *La "morte digitale",* in *Dir. inf.* (Il), 2014, 891 ss.

indisponibilità.

Con il testamento, ad esempio, si potrebbe configurare un legato di password che è un legato atipico, attraverso il quale il testatore, a mezzo dell'attribuzione diretta delle credenziali, può conferire al legatario i diritti su ciò che le credenziali stesse custodiscono; indubbio è il contenuto complesso, in quanto si caratterizza per un oggetto immediato (ovvero, le credenziali di accesso all'*account)* e un oggetto mediato (il contenuto protetto dalle *password*).

Né va sottaciuta, inoltre, per quanto riguarda l'incentivo alla redazione dei testamenti in termini di politica governativa, la posizione messicana che appare essere molto eloquente; difatti, durante il mese di settembre di ogni anno- conosciuto come mese nazionale dedicato all'atto di ultima volontà- il governo messicano promuove una campagna per incoraggiare i cittadini a fare testamento. A questi scopi, i notai offrono grandi sconti; l'obiettivo è quello di incoraggiare le persone a fare testamento e quindi pianificare la propria eredità al fine di evitare anche conflitti futuri.[25]

In questo nuovo contesto il testatore va studiato verso una riappropriazione di una funzione di catalogazione che gli appartiene in quanto titolare del bene; chi più del testatore può identificare i propri beni, stabilirne le dinamiche e le attribuzioni per il periodo *post mortem*? Consegue che forse è proprio in ordine alla cosiddetta eredità digitale che andrebbe sviluppato il dibattito sulla necessità della primazia del testamento sulla volontà statuale espressa nella successione *ab intestato*.

Ed allora torna la riflessione circa il ruolo fondamentale della figura dell'esecutore testamentario.

A sostenere – se non direttamente almeno indirettamente il ruolo decisivo dell'esecutore testamentario – a ben vedere, intervengono le stesse piattaforme *on line*: difatti molte piattaforme prevedono il caso di morte dell'utente e predispongono modelli per disattivare l'account o per eliminarne il contenuto o per indicare un nuovo utilizzatore.

Ma chi deve compiere queste attività se non un fiduciario nominato dal defunto? Le stesse piattaforme si sono in un certo qual modo organizzate, con un meccanismo di autogoverno, per la gestione dei dati digitali in caso di morte dell'utente; la rete sociale Facebook (Meta) consente al titolare dell'account di designare un <<legacy contact>>, che possa amministrare l'account dopo la morte del titolare, attraverso la stipula, on-line, di una sorta di mandato *post mortem* [26]. Va ricordato che il mandato *post mortem* è un

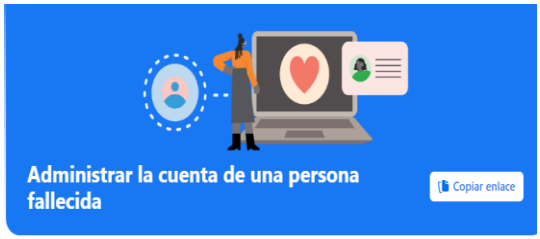
[25] Septiembre, mes del testamento 2022: cuál es la edad mínima para poder heredar en cada estado", página consultata il 4/12/2022, https://www.infobae.com/america/mexico/2022/08/26/septiembre-mes-del-testamento-2022-cual-es-la-edad-minima-para-poder-heredar-en-cada-estado/

[26] M. GALLETTI, *Mandato e regolamentazione di interessi post mortem*, in *Atti dell'Accademia peloritana dei pericolanti*, vol. LXXIII, Napoli, 2006, 233-269; il mandato *post mortem, iuvat repetere come è noto,* è un vero e proprio contratto *inter vivos*, in forza del quale il mandatario si obbliga, nei confronti del mandante, a compiere determinanti atti giuridici per conto di quest'ultimo (*ex* art. 1703 c.c.) dopo la sua morte. L'esecuzione del negozio bilaterale è differita al momento della morte del mandante e si estrinseca in un'attività materiale o in un atto esecutivo rispetto ad una attribuzione patrimoniale già realizzatasi in vita]. Trattandosi, tuttavia, di un contratto, idoneo ad incidere sull'assetto dei rapporti giuridici del *de cuius* dopo la sua morte, la dottrina si è interrogata a lungo sulla sua ammissibilità[23], sostenendo che potrà considerarsi nullo, *ex* artt. 457 e 458 c.c., il mandato attraverso il quale le parti intendano realizzare un'attribuzione patrimoniale (come consegnare al destinatario le credenziali di accesso ad un *account exchange*); diversamente, quando il mandatario debba compiere un atto a contenuto non patrimoniale

contratto tra vivi con il quale una parte si obbliga a compiere uno o più atti giuridici per conto dell'altra dopo la morte di quest'ultima; esso è valido purché l'incarico non preveda il compimento di atti dispositivi di diritti patrimoniali successori (trasferimento di beni del mandante a terzi) o di altri atti a contenuto patrimoniale. In altri termini, al mandatario viene affidato il compito di eseguire o di svolgere, dopo la morte del mandante, una mera attività materiale, eventualmente in esecuzione di un'attribuzione patrimoniale già perfetta in vita dal mandante. La circostanza che l'attività oggetto dell'incarico non abbia carattere patrimoniale esclude che il mandato possa considerarsi in contrasto con il divieto dei patti successori.

Nel caso in cui il titolare dell'account decida che il suo profilo utente duri oltre la sua morte, i suoi contatti potranno lasciare messaggi e condividere ricordi sul social network Facebook che possedeva il defunto.

In tal modo l'interessato potrà prestare il proprio consenso alla permanenza della propria immagine sull'account; pertanto, alla morte del titolare dell'account, Facebook (Meta) offre due opzioni, vale a dire la scelta di un "contatto legacy" o la cancellazione dell'account.



E La persona scelta per essere responsabile del profilo del futuro defunto dopo la sua morte è chiamata "contatto ereditario".

Il contatto dell'erede è un esecutore che può accettare richieste di amicizia per conto di un profilo commemorativo, modificare la foto del profilo e la foto di copertina.

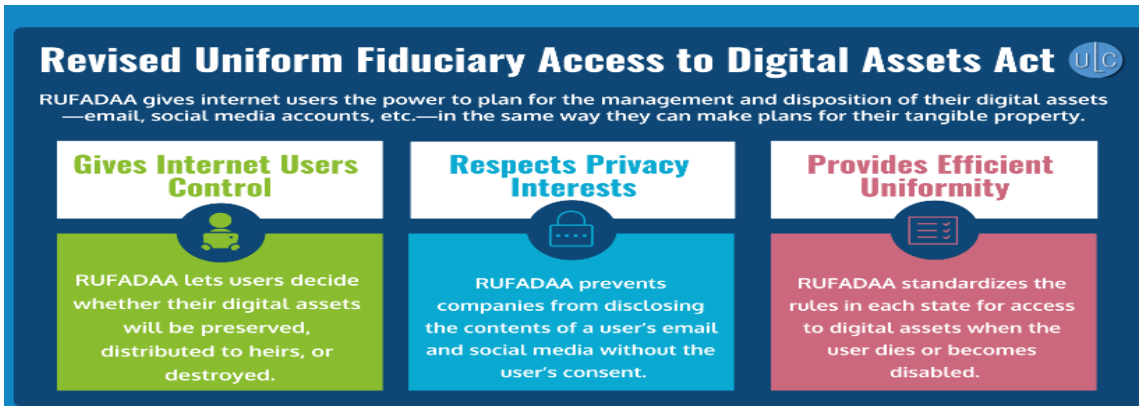
Come detto, l'esecutore (o contatto con l'erede) può anche scegliere di eliminare definitivamente l'account Facebook (Meta); selezionando quest'ultima opzione, solo il profilo principale diventerà commemorativo nel caso in cui l'azienda venga a conoscenza della morte della persona.

---

avente ad oggetto una attività materiale o marcatamente esecutiva, il mandato si considera valido. Facebook corre elriesgo de convertirse en un cementeriodigital a finales de siglo", páginacompulsadael 4/12/2022, https://www.europapress.es/portaltic/socialmedia/noticia-facebook-corre-riesgo-convertirse-cementerio-digital-finales-siglo-20190501105123.html. LAMBER, Néstor D. , "Los bienes digitales en la herencia", Publicado en: DFyP 2019 (junio), 91,Cita: TR LALEY AR/DOC/1495/2019. El art. 380 del CCCN dispone que *"El poder se extingue: a) por el cumplimiento del o de los actos encomendados en el apoderamiento; b) por la muerte del representante o del representado; sin embargo subsiste en caso de muerte del representado siempre que haya sido conferido para actos especialmente determinados y en razón de un interés legítimo que puede ser solamente del representante, de un tercero o común a representante y representado, o a representante y un tercero, o a representado y tercero …".*

Va ricordato che nel 2014 viene pubblicato l'Uniform Fiduciary Access to Digital Assets Act (UFADAA)[27] che autorizza, non solo gli amministratori dei beni della persona deceduta, ma anche i fiduciari in generale, ad accedere alle risorse digitali, salvo espressa indicazione contraria del proprietario.

L'anno successivo (2015) è pubblicato il Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), che autorizza solo i fiduciari ad accedere al catalogo delle comunicazioni elettroniche dell'utente (elenco dei messaggi inviati e ricevuti e indirizzi di posta elettronica), a meno che questo non abbia stabilito diversamente. Tuttavia, per accedere ai contenuti è necessario il consenso espresso del defunto.



In questo panorama, l'Inactive Account Manager di Facebook Legacy Contacty Google ha dato la possibilità agli utenti di designare persone che gestiranno il contenuto dei propri account in caso di morte o di inattività prolungata e, nel caso in cui nessuno di questi strumenti sia stato scelto, saranno soggetti alla volontà espressa nel testamento. Non va sottaciuto che Twitter, offre un modulo per disattivare l'account dell'utente, che deve essere accompagnato dal certificato di morte; Gmail fornisce un modulo chiamato <account manager attivo> in cui dà la possibilità di eliminare il contenuto o delegare il contenuto a dieci persone selezionate, in caso di morte del titolare dello stesso account; ELegacy consente di creare e sottoscrivere, utilizzando un sistema di documenti informatici e firme elettroniche, un mandato *post mortem exequendum* con il quale conferire al mandatario (ovvero alla società sviluppatrice) un incarico per l'esecuzione delle attività (di consegna o di cancellazione) che l'utente avrà previsto per ciascun cespite del proprio patrimonio digitale.

LegacyLocker prevede la possibilità di salvaguardare le password dei social network e delle piattaforme online che verranno consegnate alla persona designata una volta conosciuta la morte del titolare. Tellmebye aiuta a proteggere reti, cloud, file o contenuti digitali che vengono poi consegnati agli amministratori una volta notificata la malattia o la morte. La società Tellmebye chiede circa 30 euro per ricevere le ultime volontà del defunto e

[27] RUFADAA is a law that provides the Executor of an Estate, or an attorney, with access to someone's online accounts after death or incapacitation. Developed by the Uniform Law Commission (ULC), RUFADAA extends the power traditionally given to the Executor of an Estate or a Trustee when managing someone's tangible assets to include their digital assets as well.

pianificare così l'eredità digitale, fornendo informazioni agli eredi. Ma cosa potrà mai succedere se queste piattaforme gestite da società non sempre immediatamente identificate o identificabili non dovessero più esistere al momento della morte dell'utente?

Come si vede sono molte le criticità all'interno del tema in argomento che necessitano di attenzione e sensibilità perché si possa giungere ad una responsabile regolamentazione per supplire ad ogni eventuale - e più che mai possibile- mancanza di tutela della persona da parte di gestori che, fuori controllo, potrebbero non esistere più e portar via nell'oblio assoluto tantissimi dati di persone decedute neutralizzandone ogni memoria[28].

5. Profili commemorativi nelle piattaforme. Giurisprudenza tedesca, giurisprudenza americana.

Altro aspetto interessante che coinvolge l'utilizzo dei social è quello strettamente commemorativo offerto ad amici e familiari del defunto; una sorta di luogo virtuale in cui riunirsi e condividere i ricordi di una persona cara deceduta, esercitando così il cosiddetto "diritto alla memoria", come afferma Eneko Delgado.[29]

Le loro caratteristiche sono: La frase *In memoria di …* appare accanto al nome della persona nel suo profilo; a seconda delle impostazioni sulla privacy del profilo, gli amici possono condividere ricordi nella sequenza temporale del memoriale; I profili commemorativi non vengono visualizzati nei suggerimenti, nei promemoria dei compleanni o negli annunci di "persone che potresti conoscere"; nessuno può accedere a un *account* del profilo commemorativo; i profili commemorativi che non hanno un *contatto erede* non possono essere modificati.

Tuttavia, se la società che fornisce il servizio non viene informata della morte del titolare e "qualcuno" dovesse continuare ad accedervi con la propria password, cosa vietata anche se si tratta di eredi, si potrebbe

---

[28] O. LEON, *Derecho e identidad digital post-mortem*, publicado en *Testamento ¿Digital?, Desafíos legales*, septiembre 2016,76, chrome-extension://ieepebpjnkhaiioojkepfniodjmjjihl/data/pdf.js/web/viewer.html?file=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Flibro%2F657167.pdf, página compulsada el 4/12/2022.
C. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf.*, 2018, 65 rileva che "in assenza di valide disposizioni testamentarie o *mortis causa* da parte del *de cuius*, la sorte dei suoi dati depositati in queste piattaforme è affidata alle clausole del contratto in precedenza sottoscritto. Agli eredi che volessero entrare in possesso di questi dati, e che si vedessero opposto un rifiuto da parte del provider, non resterebbe che un'azione giudiziaria, condotta secondo la legge regolatrice del rapporto, diretta non al subentro nel contratto, ma semmai all'accesso, al recupero e/o alla distruzione di questi dati, nell'esercizio di un interesse o di un diritto proprio alla conoscenza dei dati, ovvero a tutela della reputazione del defunto se ne ricorrono le condizioni". Cfr., anche, G. RESTA, *La "morte" digitale*, in *Dir. inf.*, 2014, 907 ss., il quale pone in luce come la maggior parte dei dati personali digitali è nella disponibilità dei *providers* e la loro (in)trasmissibilità è di base regolata nelle condizioni del contratto di servizio. Si tratta di clausole di contratti *standard* unilateralmente predisposte, spesso di diritto statunitense, e tendenzialmente orientate alla intrasferibilità dell'*account* e dei suoi contenuti.
[29] S. MOLINA PEREZ-TOMÈ, M. SANCHEZVALDEON, *La memoria defuncti y elderecho al honor post-mortem online*, publicado en *Testamento Digital*, coordinado por O. LEON, R. VALEROBANCELO, 2016, España,83, chromeextension://ieepebpjnkhaiioojkepfniodjmjjihl/data/pdf.js/web/viewer.html?file=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Flibro%2F657167.pdf, página compulsada el 21/1/2023.

configurare un reato penale; oltre al fatto che appare essere buona norma che gli eredi del titolare deceduto comunichino al social network la morte di quest'ultimo.

Nel 2012, una ragazza di 14 anni (Facebook richiede che gli utenti abbiano almeno 13-14 anni per creare un account con il consenso dei genitori) crea un account sul social network Facebook, ma l'anno successivo muore investita sui binari di un treno a Berlino. Il social network in questione, dopo essere stato informato della morte dell'adolescente, blocca il suo profilo per tutelare la privacy della giovane e crea un account commemorativo affinché parenti e amici potessero lasciare messaggi in una sezione apposita della pagina. I genitori dell'adolescente, pur essendo a conoscenza della password dell'account, non possono, però, accedervi, tanto che chiedono all'azienda di consentire loro l'accesso per cercare di chiarire le circostanze del tragico evento: il loro obiettivo era scoprire se si fosse trattato di un incidente o di un suicidio.

Di fronte al rifiuto di Facebook di fornire loro l'accesso richiesto, i genitori intentano una causa contro la società. Il Tribunale Regionale di Berlino con sentenza n. 200172/2015 (17/12/2015) analizza le norme applicabili per verificare se i genitori avessero il diritto di accedere al profilo social della figlia e stabilisce il legittimo interesse dei ricorrenti a conoscere le informazioni contenute nell'account della figlia defunta, ragion per cui accoglie la domanda e, per l'effetto, ordina a Facebook che ai genitori venisse consentito l'accesso, a maggior ragione perché genitori sono rappresentanti legali e, in quanto eredi del patrimonio digitale della figlia, hanno diritto alla verità attraverso la conoscenza delle informazioni contenute nel profilo della giovane.

Nel maggio 2016, però, a seguito dell'approvazione del Regolamento generale europeo sulla protezione dei dati, Facebook, viste le norme relative alla tutela della privacy di terzi, impugna la sentenza innanzi al Tribunale Federale di Berlino, sostenendo la complessità della vicenda e la priorità della protezione della privacy del terzo (titolare account e utenti in connessione), pur manifestando comprensione ed empatia con la famiglia della ragazza deceduta.

In data 7/12/2018 Il Tribunale Federale di Berlino revoca la sentenza di primo grado considerando prioritaria la tutela della privacy dei terzi, in forza di quanto previsto dal citato Regolamento; la segretezza delle comunicazioni digitali (o corrispondenza digitale) è garantita dalla Legge Fondamentale tedesca e si applica anche ai contenuti dell'account Facebook.

Visto l'esito sfavorevole, i genitori impugnano la sentenza davanti alla Corte Suprema Federale di Giustizia di Karlsruhe (BGH), invocando, in modo inedito, il diritto all'eredità digitale che, a loro avviso, prevaleva sul diritto alla privacy.

La Corte accoglie le doglianze dei ricorrenti e afferma che l'account era un mezzo sociale ereditabile allo stesso modo della corrispondenza: gli eredi hanno il diritto di accedere all'account Facebook dei loro parenti defunti e, pertanto, l'ufficio giudiziario dichiara nulla la condizione generale contenuta nel contratto di adesione stipulato dal suddetto social network nella parte in cui vieta l’accesso.

Nel 2017 il Parlamento tedesco aveva già approvato la legge federale sulla protezione dei dati (BDGS) che è conforme alle disposizioni del regolamento generale europeo sulla protezione dei dati (GDPR).

Non vi è dubbio che la citata sentenza costituisca un importante precedente sulla questione affrontata, poiché la Corte Suprema tedesca stabilisce che l'account di un social network (Facebook) include beni reliquiari e allo stesso tempo indica che le condizioni generali che lo escludevano dall'eredità erano abusive e, quindi, nulle. Come è noto, le clausole abusive hanno lo scopo di rafforzare la posizione economica e giuridica del professionista che le redige, abusando della sua posizione contrattuale predominante, cosiddetta match position[30]. La necessità di realizzare quella che si potrebbe definire "salute contrattuale", nelle parole di Rezzónico, richiede la sottoposizione del contenuto delle condizioni generali di negoziazione al controllo della Magistratura per correggere o contrastare gli abusi che determinano un significativo squilibrio tra diritti e obblighi delle parti a danno del consumatore[31]; si ricorda che i principi guida che regolano l'ermeneutica di questo tipo di contratti sono la buona fede, il *favor consumatoris* e l*'interpretatio contra stipulatorem*.

Questo tipo di clausole comportano un significativo squilibrio dei diritti e degli obblighi reciproci, di portata tale da compromettere il principio di massima reciprocità degli interessi, incidendo sul rapporto di equivalenza. Si tratta di clausole gravose, oppressive, leonine, assolutamente sfavorevoli per l'aderente e irritanti per un giusto ordinamento contrattuale, in attesa di una "equità terapeutica" come dice Esser-Schmidt.

Puig Brutau afferma giustamente che il diritto contrattuale vive una vera pseudomorfosi, cioè che si tratta di una crescita solo apparente, di un tipo di ammissione solo formale come "impegno", che deriva dall'applicazione del suo significato e qualificazione in una realtà socialmente ed economicamente contrario all'essenza del diritto contrattuale. La tattica derivata dall'autoritarismo negoziale consentito del "prendere o lasciare" – che trasforma la relazione in un diktat, in cui non esiste alternativa – significa uno squilibrio di potere, poiché una delle parti impone il proprio dominio sull'altra sotto l'apparenza della forma giuridica "contratto".[32]

Tornando al caso citato, finalmente, dopo cinque anni e mezzo, i genitori hanno potuto accedere all'account Facebook della figlia defunta.[33]

Alla luce delle argomentazioni addotte, si può dedurre che, poiché gli eredi rivestono la qualità di successori dei rapporti giuridici del defunto, hanno diritto di accesso al contenuto delle loro email poiché ritengono tali beni suscettibili di essere trasmessi mortis causa. Tuttavia, non ignoriamo il fatto che ciò potrebbe avere un impatto sul diritto alla privacy di terzi che meritano anch'essi protezione.

John Ellsworth, il padre di un marine di 20 anni la cui morte è avvenuta in Iraq quando è esplosa la bomba che stava cercando di disinnescare, chiede a

---

[30] G. ZAPA, *Régimen de las cláusulas abusivas en la Ley de Defensa del Consumidor*, publicado en *Manual de Defensa del Consumidor*, G.STIGLITZ, ed. Juris, Rosario, 2004, 139.

[31] J.REZZONICO, *Contratos con cláusulas predispuestas*, Astrea, Buenos Aires, 1987, 11.

[32] J. REZZONICO, *Contratos con cláusulas predispuestas*, Astrea, Buenos Aires, 1987, 320-321.

[33] *Para la Justicia alemana, las cuentas en redes se heredan*, página compulsada el 1/12/2022https://comercioyjusticia.info/justicia/para-la-justicia-alemana-las-cuentas-en-redes-se-heredan/.

Yahoo di consegnare il contenuto dell'account di posta elettronica di suo figlio Justin Ellsworth. L'azienda respinge la richiesta, sostenendo che il servizio era stato pensato proprio per tutelare la privacy dell'utente vietandone l'accesso a terzi dopo la morte del titolare; Yahoo, in definitiva, sostiene che l'Electronic Communications Privacy Act del 1986 proibisca la divulgazione delle comunicazioni personali degli utenti senza un ordine del tribunale.

Il signor Ellsworth in quanto erede insiste affinché gli venga riconosciuto il diritto di accedere all'account, comprese le e-mail inviate e ricevute; tuttavia, secondo la politica di Yahoo, l'azienda potrebbe cancellare l'account in questione nonostante sia in contrasto con la volontà del padre del giovane soldato defunto.

Alla fine, il magistrato approva la politica sulla privacy di Yahoo, ma ordina al suddetto motore di ricerca di fornire all'attore un CD contenente una copia delle e-mail provenienti dall'account in questione.

A questo proposito, Martín A. Floresse si chiede quale regime giuridico possa spiegare questo risultato[34] e fornisce una possibile interpretazione: Yahoo possedeva le copie delle email archiviate sui suoi server e, in quanto proprietario delle email, doveva consegnarne una copia. Pertanto, il soldato estinto sarebbe titolare dei diritti d'autore, poi trasferiti agli eredi; una seconda interpretazione è quella di considerare il giovane defunto come il proprietario delle email che mentre era in vita venivano trasmesse mortis causa agli eredi. L'autore citato evidenzia che questa interpretazione è meno realizzabile perché il tribunale avrebbe allora ritenuto che i diritti degli eredi fossero superiori ai termini e alle condizioni del contratto stipulato dal defunto, ordinando il pieno accesso all'account. Tuttavia, il tribunale ordina a Yahoo solo di rivelare il contenuto delle e-mail, ragion per cui si conclude che la società era proprietaria del conto mentre gli eredi avevano il diritto di accedere al contenuto delle e-mail.

John Ellsworth in un'intervista alla radio di Detroit WJR afferma che Yahoo ha agito in modo responsabile dopo la sentenza e aggiunge che il padre del giovane morto è stato anche aiutato, dalla stessa azienda, a decifrare le informazioni contenute nel CD[35].

Vale la pena notare che il tribunale ha omesso di pronunciarsi in questa sentenza del 2005 su chi fosse il proprietario del contenuto dell'e-mail poiché ha concentrato la sua analisi sul diritto alla privacy.

La madre di una famosa modella, SaharDaftary, morta a Manchester dopo essere caduta intenzionalmente dal dodicesimo piano dell'appartamento di proprietà del marito Rashid Jamil, un promotore immobiliare, ha cercato di accedere all'account della figlia per scoprire la verità sui fatti accaduti; ella era a conoscenza del fatto che sua figlia utilizzava regolarmente il social network Facebook e riteneva che non si fosse trattato di suicidio. Poco dopo il triste episodio, la polizia britannica aveva arrestato Jamil con l'accusa di omicidio; secondo le indagini del medico legale, è stato riferito che Jamil aveva

[34] M. A. FLORES, *Herencia Digital: Un nuevo desafío para el derecho sucesorio*, Publicado en: DFyP 2020 (junio), 143, Cita: TR LALEY AR/DOC/3253/2019.

[35]"Yahoo releases e-mail of deceased Marine",https://www.cnet.com/tech/tech-industry/yahoo-releases-e-mail-of-deceased-marine/, página compulsada el 4/12/2022.

violentato sua moglie SaharDaftary.

La Corte ha affermato che le comunicazioni archiviate rientrano nel diritto alla privacy che tutela le comunicazioni e i contenuti degli account e, pertanto, la società Facebook non può essere costretta a fornire i contenuti[36].

La giurisprudenza è ondivaga; le sentenze sopra richiamate rivelano le diverse posizioni della magistratura nei diversi Paesi quando si tratta di risolvere i conflitti relativi alle informazioni contenute nei social network come Facebook dopo la morte della persona. Per questo motivo è opportuno approfondire lo studio dell'eredità digitale e successivamente regolamentarla normativamente.

6. Qualche conclusione.

Parlare di eredità digitale non è cosa semplice, ma giusta.[37]

Il giurista non può esimersi dal controllo delle mutazioni sociali che si traducono in nuove istanze.

Di certo quello che rileva è che non tutto ciò che appare sussumibile nella valigia del concetto ellittico di eredità digitale diventa, *sic et simpliciter*, patrimonio ereditario.

Il patrimonio ereditario, a voler utilizzare una metafora, è un bagaglio a mano, non una valigia in cui introdurre tutti i diritti che non sempre hanno carattere della trasmissibilità.

Il problema esiste e sarà sempre più tangibile soprattutto in assenza di una legislazione *ad hoc* stante il pur troppo ampio spazio di intervento, con le relative criticità, alle diverse impostazioni giurisprudenziali che non possono sostituire "la regola derivante dal diritto positivo", né appare possibile lasciare un mercato incontrollato di morti digitali nella gestione libera di piattaforme[38].

Sta di fatto che anche in questo nuovo contesto il testamento finisce con l'essere una più che sostenibile soluzione in quanto finisce con l'assumere una posizione di forte rilievo: è il testatore, con la sua autonomia, a decidere come

---

[36]N. MORALEJO IMBERNON, *El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, chrome-extension://ieepebpjnkhaiioojkepfniodjmjjihl/data/pdf.js/web/viewer.html?file=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F7504469.pdf., página compulsada el 4/12/2022.

[37]Per un approfondimento sulla componente digitale del patrimonio del de cuius cfr. A. MOLLO, *Eredità digitale e piattaforme online. Tutela e profili di pianificazione*, Napoli,2021, *passim*; A. MOLLO, *La successione a causa di morte e le nuove tecnologie digitali*, in L. GATT (a cura di) Atti del convegno di Napoli *Il diritto di famiglia e dei minori nell'era digitale*, Pisa, 2021.

[38]C. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf.*, 2018, 65 rileva che "in assenza di valide disposizioni testamentarie o *mortis causa* da parte del *de cuius*, la sorte dei suoi dati depositati in queste piattaforme è affidata alle clausole del contratto in precedenza sottoscritto. Agli eredi che volessero entrare in possesso di questi dati, e che si vedessero opposto un rifiuto da parte del provider, non resterebbe che un'azione giudiziaria, condotta secondo la legge regolatrice del rapporto, diretta non al subentro nel contratto, ma semmai all'accesso, al recupero e/o alla distruzione di questi dati, nell'esercizio di un interesse o di un diritto proprio alla conoscenza dei dati, ovvero a tutela della reputazione del defunto se ne ricorrono le condizioni". Cfr., anche, G. RESTA, *La "morte" digitale*, in *Dir. inf.*, 2014, 907 ss., il quale pone in luce come la maggior parte dei dati personali digitali è nella disponibilità dei *providers* e la loro (in)trasmissibilità è di base regolata nelle condizioni del contratto di servizio. Si tratta di clausole di contratti *standard* unilateralmente predisposte, spesso di diritto statunitense, e tendenzialmente orientate alla intrasferibilità dell'*account* e dei suoi contenuti.

e a chi attribuire i suoi beni digitali; come è al testatore che compete il compito di individuare specificamente i beni digitali di cui ha disponibilità e volere di trasmetterli.

Va aggiunto che, poiché l'eredità digitale appare priva di regolamentazione, gli eredi o i legatari non hanno a disposizione gli strumenti adeguati per determinare e identificare le risorse digitali o per proteggere l'identità digitale *post mortem* del defunto nel cyberspazio, e men che meno possono controllare la gestione di società che non si sa per quanto tempo ed in che modo offrono i propri servizi. Né è escluso il pericolo di un mercato nero delle identità *on-line* in cui chiunque potrebbe acquistare identità vere o false all'asta.

Queste riflessioni inducono a sottolineare ancora il fondamentale ruolo della figura dell'esecutore testamentario, *longa manus* del defunto per gestire al meglio e per tutelarne in modo sostanziale l'eredità digitale, sia sotto il profilo economico, sia sotto il più circoscritto ambito personalistico.

L'urgenza del testamento in tema di digitalizzazione esige una attenzione massima. Affrontare questo tema in modo approfondito e regolamentare la successione digitale tenendo conto di un bilanciamento tra norme di ordine pubblico del diritto successorio e norme sulla tutela dei dati personali e sul diritto alla privacy dei terzi, è cosa indispensabile, soprattutto se si tiene conto che alcune piattaforme digitali consentono la designazione di figure quali *legacy contact* non previste e che potrebbero nascondere insidie e pericoli non solo per la memoria del defunto, ma anche per il corretto ambito e l'esecuzione dei diritti successori.

Né appare peregrina la preoccupazione della omessa trasparenza sulla garanzia che deve fornire la piattaforma circa la conservazione corretta dell'eredità digitale del defunto e del tempo previsto; preoccupazione che il giurista ha il compito di avere anche in una prospettiva etica di questa indagine.

Ed allora, se come afferma Guido Alpa, la globalizzazione e la rivoluzione digitale offrono al giurista materiale per riformulare gli schemi tradizionali del diritto privato, riorganizzare l'attività stessa, promuovere i valori della persona[39], non va trascurato che è proprio il valore della persona che deve emergere in una società antropocentrica: e se dal generico – e non sempre comprensibile – *interesse* di mercato si passa al valore umano, la tutela del diritto di fare testamento non potrà giammai soggiacere alle leggi economiche delle piattaforme on-line.

[39] G. ALPA, citato da P. N. Guerreiro, *Incumplimiento obligacional en el comercio digital. Tutela de la debilidad negocial*, EBOOK-TR 2022 (Alterini), 543; TR LALEY AR/DOC/1255/2022.

SECTION II

FOCUS PAPERS

Altieri A, 'Lo stato di automazione del processo civile e delle procedure concorsuali nell'interazione tra parti pubbliche e private' (2023) 2 EJPLT, 187 - 216.
DOI: https://doi.org/10.57230/EJPLT223AA

EJPLT
ISSN 2704-8012



Lo stato di automazione del processo civile e delle procedure concorsuali nell'interazione tra parti pubbliche e private

The progress of automation of civil and insolvency proceedings in the interaction between public and private actors

ATTILIO ALTIERI
Research Fellow in Business Law, University of Foggia, Italy

Abstract

Il contributo si propone di indagare i meccanismi di automazione nel processo civile nelle procedure concorsuali, attraverso l'analisi della normativa di riferimento sia del processo telematico che del Codice della crisi d'impresa e dell'insolvenza. A tal fine, si prenderà in considerazione il grado di automazione dei procedimenti, evidenziandone le criticità e le funzioni non ancora implementate; si procederà inoltre ad una comparazione con i sistemi processuali di Germania, Francia e Spagna; si tratteggeranno infine le conclusioni in vista di prospettive future utili ad una maggiore armonizzazione tra procedimenti giurisdizionali e tecnologia.

The paper aims to investigate the mechanisms of automation in civil and insolvency procedures, through the analysis of the reference legislation of both the telematic process and the New Insolvency Law. To this end, the degree of automation of proceedings will be taken into consideration, highlighting critical issues and functions not yet implemented; a comparison will be made with the procedural systems of Germany, France and Spain; conclusions will be drawn in view of future outlooks useful for a greater harmonisation between judicial proceedings and technology.

© The author(s) 2023, 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: Civil trial; Artificial Intelligence; insolvency law; telematic trial; automation of proceedings; technology.

Sommario: 1. Premessa. – 1.1. La disciplina del processo telematico. – 1.2. La normativa secondaria. – 2. Il processo telematico nel Codice della crisi. – 3. Lo stato di attuazione. – 4. Funzionalità non implementate e criticità. – 5. Analisi comparata nei principali paesi UE. – 5.1. Germania. – 5.2. Francia. – 5.3. Spagna. – 6. Prospettive future.

1. Premessa[1].

L'avvento della tecnologia ed in particolare dell'Intelligenza Artificiale ha comportato diversi cambiamenti in tutto il settore legale. Basti pensare che il "*2023 Future Ready Lawyer Survey Report*"[2], nell'analisi della situazione dei professionisti del settore legale a livello globale, individua, tra i trend più significativi, l'impiego delle tecnologie e dell'AI negli studi legali: infatti, il 73% degli avvocati intervistati ha affermato che utilizzerà nei prossimi dodici mesi l'intelligenza artificiale generativa; mentre una maggioranza significativa (91%) ritiene importante disporre di tecnologie che permettano agli avvocati di adattarsi rapidamente ai cambiamenti, avere accesso a strumenti e tecnologie più avanzati che favoriscano la produttività e permettano di adottare processi basati sull'uso delle tecnologie. In un quadro così composto si inserisce appieno lo stato di automazione del processo civile e delle procedure concorsuali (ed eventualmente delle altre procedure in seno al processo civile, come ad esempio i sequestri), che consente un'interazione tra ausiliario del giudice (curatore, custode, amministratore giudiziario), giudice e avvocati, sempre più mediata dalla tecnica. Al fine di condurre tale analisi, si partirà dalla normativa di riferimento che riguarda l'introduzione del processo telematico nel nostro ordinamento e, successivamente, che ha interessato più da vicino il Codice della crisi d'impresa e dell'insolvenza (d.lg. 12 gennaio 2019, n. 14, d'ora in poi c.c.i.), considerando anche la normativa di matrice regolamentare; la ricerca proseguirà guardando al sistema nel suo complesso e, in particolare, all'attualità del grado di automazione; si affronteranno le criticità e le funzioni non ancora implementate; si procederà ad una comparazione con i sistemi processuali della Germania, della Francia e della Spagna; infine si tratteggeranno le conclusioni in vista di prospettive future utili ad una maggiore armonizzazione tra procedimenti giurisdizionali e tecnologia.

1.1. La disciplina del processo telematico.

Il processo civile telematico (abbreviato anche in PCT), il cui concreto avvio

[1] Questa pubblicazione è stata realizzata nell'ambito del Programma PRIN 2017, Progetto di ricerca di Rilevante Interesse Nazionale: "Artificial Intelligence and Legal Studies Perspectives. Are the Algorithmic decision-making and data driven predictions calling for a new legal framework? A focus on financial and labour markets highlighting protection of rights and wealth distribution", Prot. 2017L9HJ25_001, CUP I84I19001180008.

[2] Consultabile al sito: https://www.wolterskluwer.com/en/know/future-ready-lawyer-2023.

si deve all'introduzione delle disposizioni in tema di esclusività del deposito mediante invio telematico di taluni atti c.d. endoprocessuali[3], come è noto, è funzionante dal 30 giugno 2014. È altrettanto noto che esso si fonda su una infrastruttura risalente agli anni 2000[4] e che nel corso del tempo si sono registrate varie ragioni per la lentezza nell'attuazione concreta di principi già stabiliti tempo addietro[5]. La pandemia da Covid-19 e il PNRR hanno rappresentato il volano, tra l'altro[6], per la modifica delle Disposizioni per l'attuazione del codice di procedura civile, cui è stato aggiunto il Titolo V *ter* – Disposizioni relative alla giustizia digitale. Le norme in esso contenute e, più in generale, quelle presenti in tutto il decreto legislativo 149/2022, hanno il duplice scopo di confermare, da una parte, gli interventi presi durante la pandemia da Covid-19 e, dall'altra, quella di introdurre ulteriori novità[7]. La l. 29 dicembre 2022, n. 197 (legge di bilancio) con l'art. 1 comma 380 lettera a, ha apportato modifiche all'art. 35, d.lg. n. 149/2022 modificando l'entrata in vigore di alcune delle disposizioni del decreto legislativo 149/2022,

[3] V. art. 16 *bis*, d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 221 e poi integrato dall'art. 1, comma 19, punto 2, l. 24 dicembre 2012, n. 228. Il successivo d.l. n. 90 del 2014 (convertito dalla l. n. 114 del 2014) precisò poi che l'obbligo del deposito telematico avrebbe interessato esclusivamente i procedimenti iniziati davanti al tribunale ordinario a partire dal 30 giugno 2014; mentre per quelli avanti alle corti d'appello si sarebbe dovuto attendere l'anno successivo. Ancora il d.l. n. 83 del 2015 (convertito dalla l. n. 132 del 2015) ha ammesso, nell'àmbito dei procedimenti civili contenziosi e di volontaria giurisdizione, innanzi al tribunale e alla corte d'appello, il deposito telematico di qualsiasi atto del processo, non solo endoprocessuale, così risolvendo le discrasie createsi nella giurisprudenza di merito in ordine alla validità del deposito telematico degli atti introduttivi del giudizio.

[4] Il Ministero della giustizia ha cominciato a lavorare al progetto del PCT dal 1997, ma solo con il d.p.r. n. 123 del 2001 (primo regolamento recante la "disciplina sull'uso di strumenti informatici e telematici nel processo civile") è stata definita la struttura tecnica e normativa dei servizi informatici della giustizia civile. La normativa dettata da questo provvedimento è stata il primo esempio applicato – seppur parzialmente – di digitalizzazione di un ampio settore della p.a. ed ha rappresentato un punto di riferimento per tutti i futuri programmi e progetti di informatizzazione nel settore pubblico in quanto in esso, per la prima volta, si affermava che: "È ammessa la formazione, la comunicazione e la notificazione di atti del processo civile mediante documenti informatici" e che "L'attività di trasmissione, comunicazione o notificazione dei documenti informatici, è effettuata per via telematica attraverso il sistema informatico civile". Sul punto, cfr. G.G. POLI, *Il processo civile telematico e il dialogo tra le sue fonti*, in G. RUFFINI (a cura di), *Il processo telematico nel sistema del diritto processuale civile*, Milano, 2019, 1 ss., spec. 2 nt. 3, 23 ss.

[5] Sul punto, si rinvia a B. BRUNELLI, *Il processo civile telematico che verrà*, in *Riv. trim dir. e proc. civ.*, 2021, 4, 957 ss., spec. 958 ss., dove afferma: «Per molto, troppo tempo, la digitalizzazione della giustizia è stata contrastata da numerosi operatori delle diverse categorie interessate, risoluti nel mantenere fermi gli elementi tradizionali della cultura e dell'organizzazione della giurisdizione, lasciando così che le innovazioni tecnologiche invecchiassero prima ancora di cominciare ad essere utilizzate. Mancava, d'altra parte, specie nel primo decennio degli anni Duemila, un piano complessivo e sinergico che declinasse su più dimensioni una vera prospettiva di trasformazione digitale: si continuava a girare a vuoto, pur se gli interventi legislativi si susseguivano con un ritmo quasi vorticoso»; cfr. anche A. TEDOLDI, *Il processo civile telematico tra* logos *e* techne, in *Riv. dir. proc.*, 2021, 3, p. 843 ss.; C. PUNZI, *Sul processo civile telematico*, in *Riv. dir. processuale*, 2022, 1, 1 ss.; P. BIAVATI, *La riforma del processo civile: motivazioni e limiti*, in *Riv. trim. dir. e proc. civ.*, 2022, 1, 45 ss.

[6] L'*iter* legislativo è stato caratterizzato dapprima, (nella XVIII legislatura), dall'introduzione del d.d.l. n. 1662 (presentato al Senato il 9 gennaio 2020 e divenuto d.d.l. delega 1662/S/XVIII, approvato dal Senato il 21 settembre 2021 e poi diventato definitivo a seguito della fiducia votata dalla Camera il 24 novembre 2021). Successivamente, la relativa legge (6 novembre 2021, n. 206) è stata pubblicata sulla Gazzetta Ufficiale del 9 dicembre 2021. Il d.lg. n. 149/2022 ha dato attuazione alla legge delega n. 206/2021 di riforma del processo civile.

[7] Il d.lg. 10 ottobre 2022, n. 149 impatta la disciplina degli ADR, mediazione, negoziazione e arbitrato, tocca alcune norme delle disposizioni generali, ridisegna il rito ordinario, gli affianca il nuovo procedimento semplificato di cognizione, interviene sulle impugnazioni, introduce due nuovi istituti, il rinvio pregiudiziale alla Corte di cassazione e la revocazione delle decisioni dichiarate contrarie alla CEDU, inserisce nel libro secondo del codice di rito il nuovo titolo IV-*bis*, relativo al procedimento in materia di persone, minorenni e famiglie, si occupa del processo esecutivo e non dimentica le disposizioni di attuazione, né altre previsioni sparse contenute nel codice civile e in leggi speciali.

anticipandole dal 30 giugno 2023 al 28 febbraio[8].

Procedendo con ordine e tentando, seppur brevemente, di organizzare le fonti (sia in senso sincronico che diacronico) che hanno caratterizzato la nascita e lo sviluppo del PCT, sembra potersi affermare che la progressiva applicazione al processo delle innovazioni informatiche e tecnologiche, voluta dal legislatore, ha avuto un notevole impatto in particolare sulla disciplina degli atti e sulla loro forma, essendo stata prevista la possibilità (e in molti casi l'obbligo) che gli atti processuali siano posti in essere in modalità dematerializzata e con l'ausilio di sistemi informatici e di trasmissione a distanza, ossia in modalità telematica. Ciò ha determinato considerevoli vantaggi (tra cui la possibilità di depositare atti processuali e documenti e di estrarne copie da remoto, la tendenziale assenza di limitazioni orarie, il risparmio di carta) ma anche una serie di criticità, derivanti sia da aspetti strettamente tecnici, sia da una copiosa produzione normativa.

Tale percorso – inizialmente avviato con il già ricordato d.p.r. n. 123/2001 – è stato progressivamente sviluppato con una successione di interventi per lo più

[8] In particolare, la digitalizzazione del procedimento in tutte le sue fasi ha comportato l'introduzione di istituti "nuovi", tra cui i principali sono: l'obbligo di deposito telematico di atti (anche introduttivi) e documenti per Tribunale, Corte d'appello, Cassazione (dal 1° gennaio 2023) (v. art. 196 *quater* disp. att. trans. c.p.c., introdotto da art. 4, comma 12, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n.149/2022 come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022); la redazione dell'atto processuale in formato digitale (e suo deposito nel fascicolo telematico) da parte di magistrati, personale degli uffici giudiziari e degli uffici notificazioni, esecuzioni e protesti (dal 1° gennaio 2023) (v. art. 196 *quinquies* disp. att. trans. c.p.c., introdotto da art. 4, comma 12, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n. 149/2022 come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022); il perfezionamento del deposito telematico con la generazione della ricevuta ed entro la fine del giorno di scadenza (dal 1° gennaio 2023) (v. art. 196 *sexies* disp. att. trans. c.p.c., introdotto da art. 4, comma 12, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n.149/2022 come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022); l'acquisizione di copia cartacea e per la riproduzione su supporto analogico degli atti depositati con modalità telematiche nonché per la gestione e la conservazione delle copie cartacee (da stabilire con decreto del Ministro della giustizia) (dal 1° gennaio 2023) (v. art. 196 *septies* disp. att. trans. c.p.c., introdotto dall'art. 4, comma 12, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n. 149/2022 come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022); l'udienza a distanza con collegamento audiovisivo (facoltativo o richiesto dal giudice) per Tribunale, Corte d'appello, Cassazione, Giudice di Pace e Trib. Sup. Acque Pubbliche (dal 1° gennaio 2023) (v. art. 196 *duodecies* disp. att. trans. c.p.c., introdotto dall'art. 4, comma 12, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n.149/2022 come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022; v. anche art. 127 *bis* c.p.c., inserito dall'art. 3, comma 10, lett. b, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n.149/2022, come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022); la trattazione scritta e deposito di note scritte in sostituzione dell'udienza, per le udienze che non richiedano la presenza di soggetti diversi da: difensori, parti, PM e ausiliari del giudice (facoltativo) per Tribunale, Corte d'appello, Cassazione, Giudice di Pace e Trib. Sup. Acque Pubbliche (dal 1° gennaio 2023) (v. art. 127 *ter* c.p.c., inserito dall'art. 3, comma 10, lett. b, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n.149/2022, come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022); la mediazione telematica e la redazione e sottoscrizione digitale del verbale informatico degli incontri tenuti con tale modalità (dal 28 febbraio 2023) (v. art. 8 *bis* d.lg. n. 28/2010); il deposito telematico degli atti e suo perfezionamento nel caso di dipendenti della PA che stanno in giudizio personalmente (dal 28 febbraio 2023) (v. art. 196 *quater* e 196 *sexies* disp. att. trans. c.p.c.); il pagamento telematico del CU e dell'anticipazione forfettaria (dal 28 febbraio 2023) (v. art. 221, comma 3, secondo periodo, d.l.n. 34/2020); la formula esecutiva telematica (dal 28 febbraio 2023) (v. art. 23, comma 9 *bis* d.l. n.137/2020); il potere di attestazione di conformità di copie di atti e provvedimenti e modalità di attestazione (in vigore esclusivamente per i procedimenti iniziati successivamente al 28 febbraio 2023) (v. art. 196 *nonies* disp. att. c.p.c., art. 196 *decies* disp. att. c.p.c., art. 196 *undecies* disp. att. c.p.c.); l'obbligo di deposito in telematico di atti e documenti per Giudice di Pace e Trib. Sup. Acque Pubbliche (dal 30 giugno 2023) (v. art. 196 *quater* disp. att. trans. c.p.c., introdotto dall'art. 4, comma 12, d.lg. n. 149/2022; per la disciplina transitoria v. art. 35 d.lg. n.149/2022 come mod. dall'art. 1, c. 380, lett. a, l. n. 197/2022); il giuramento scritto del CTU, firmato digitalmente da depositare nel fascicolo telematico (dal 30 giugno 2023) (v. art. 193, comma 2, c.p.c.; art. 221, comma 8, d.l. n.34/2020); la notificazione tramite UNEP (residuale dopo aver tentato personalmente la notificazione via PEC) (dal 30 giugno 2023) (v. art. 137 c.p.c.).

disorganici e frastagliati, affidati a fonti di rango diverso [9]. A essi deve aggiungersi anche la legislazione emergenziale legata alla pandemia da Covid-19. Tale stratificazione di norme, non del tutto ordinata e razionalizzata[10], ha condotto alla disciplina del cosiddetto processo civile telematico[11].

Il PCT, come è stato autorevolmente affermato, «non costituisce una modalità di svolgimento del processo, aggiuntiva, parallela e staccata da quella legata alla dimensione fisica o cartacea; né dovrebbe risolversi in una modalità processuale caratterizzata esclusivamente da forme dematerializzate e telematiche, quale primo passo verso inquietanti scenari – cui è aliena la giustizia – nei quali sia bandita dal processo ogni ipotesi di interazione dialogica e di svolgimento del contraddittorio in presenza e in cui si pretenda di praticare la sostituzione della intelligenza umana con le macchine»[12].

In realtà, nel suo significato più semplice, la locuzione "processo civile telematico" dovrebbe descrivere lo svolgimento di una serie procedimentale, nella quale gli strumenti tecnologici offrono utili funzionalità ai vari soggetti del processo e nella quale le prescrizioni di forme dematerializzate e telematiche dovrebbero sempre rispondere al principio di congruità e idoneità allo scopo. Quindi, le disposizioni relative al PCT sono tutte quelle che si occupano di disciplinare tale fenomeno e che necessitano di un raccordo sistematico con le altre disposizioni processuali, il più delle volte preesistenti[13].

---

[9] Tra cui si ricordano: il d.l. n. 193/2009; il d.m. n. 44/2011 (contenente le "regole tecniche" per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione); il d.l. n. 179/2012 e successive modificazioni, che ha inciso anche sulla l. n. 53/1994 relativa alle notificazioni degli avvocati; il decreto della Direzione generale per i sistemi informativi automatizzati del Ministero della giustizia 16 aprile 2014 e successive modifiche (contenente le "specifiche tecniche" del processo telematico, previste dall'art. 34, co. 1, d.m. n. 44/2011); il d.lg. n. 149/2022, con il quale sono state abrogate o novellate disposizioni precedenti nonché introdotte nuove disposizioni, anche nel codice di rito, alcune delle quali rinviano alla futura emanazione di normative tecniche di rango secondario; il d.l. n. 13/2023; la l. n. 87/2023.

[10] In tal senso, cfr. ancora G. Ruffini (a cura di), *Il processo telematico nel sistema del diritto processuale civile*, cit., *passim*; ma, da ultimo, Id. (a cura di), *Diritto processuale civile*, vol. I, *La giustizia civile*, Bologna, 2023, 171 ss.

[11] Ossia all'insieme di previsioni concernenti: la creazione di atti processuali o di copie degli stessi in "formato digitale" (sostituendo il supporto cartaceo con quello informatico); il compimento in modalità (o forma) telematica, cioè dematerializzata e con trasmissione a distanza, delle comunicazioni di cancelleria, modalità tendenzialmente prevista come esclusiva; il compimento in modalità (o forma) telematica delle notificazioni, modalità divenuta prevalente, pur permanendo ambiti di applicabilità delle notifiche tradizionali cartacee, ai sensi degli artt. 138 ss. c.p.c.; il compimento in modalità (o forma) telematica del deposito, modalità di cui si è progressivamente estesa la obbligatorietà a tutti gli atti processuali, pressoché dinanzi a tutti gli uffici giudiziari e tendenzialmente per tutti i soggetti del processo, anche se permangono ipotesi di compimento del deposito in forma tradizionale; l'obbligatoria creazione di fascicoli informatici per l'inserimento, la conservazione dematerializzata, l'accessibilità e la consultazione da remoto degli atti processuali, dei provvedimenti e dei documenti probatori; l'estrazione, anche da remoto, di copie aventi valore legale; il pagamento mediante transazione telematica, del contributo unificato e degli altri diritti dovuti per l'accesso al servizio "giustizia"; la possibilità che l'udienza possa tenersi a distanza mediante collegamento audiovisivo (art. 127 bis c.p.c.) oppure essere sostituita dal deposito telematico di atti scritti (art. 127 ter c.p.c.).

[12] G. Ruffini (a cura di), *Diritto processuale civile*, vol. I, *La giustizia civile*, cit., 172.

[13] Cfr. G.G. Poli, *Il processo civile telematico e il dialogo tra le sue fonti*, cit., 1 ss., spec. nt. 2 e la bibliografia ivi richiamata. Lo stesso A. afferma (pp. 1-3) che «la locuzione [processo civile telematico] non deve far pensare ad una nuova (futuribile) forma di processo civile, in cui il *computer* soppianta l'attività defensionale delle parti o assolve al posto del giudice il dovere decisorio attraverso l'utilizzo di algoritmi o l'elaborazione dei c.d. *big data*, ma neppure ad un nuovo modello processuale che si affianchi ai numerosi già esistenti. A quella definizione deve ancora assegnarsi, più modestamente, nonostante siano trascorsi ormai più di tre lustri dalla emanazione della prima disciplina organica (se pur sperimentale e facoltativa) del PCT, il compito di individuare una modalità di gestione in forma dematerializzata, con il *bit* invece che con la carta, mediante documento informatico invece che analogico, "da remoto" invece che "in presenza", di alcune delle relazioni

Ad oggi, come è noto, lo strumento tecnico cui è stata affidata dal legislatore la trasmissione telematica a fini di comunicazione e notificazione di atti, nonché per il deposito, ad opera dei difensori, degli atti presso gli uffici giudiziari, è la posta elettronica certificata (laddove il deposito telematico dei provvedimenti del giudice avviene con un mezzo di trasmissione diretta, denominato canale sicuro).

Sempre sul piano tecnico, inoltre, la gestione da parte del Ministero della giustizia in via informatica e telematica di attività, dati, servizi, comunicazioni è stata resa possibile mediante la creazione del "dominio giustizia", quale insieme delle risorse *hardware* e *software*, le cui funzionalità sono accessibili, per i soggetti esterni, tramite il portale dei servizi telematici o tramite i punti di accesso normati dalle disposizioni regolamentari[14]. Il sistema informatico del dominio giustizia, che consente l'interscambio di informazioni e servizi tra i soggetti interni agli uffici giudiziari (giudice e altri organi giudiziari), i soggetti esterni, il portale dei servizi telematici e i gestori di posta elettronica certificata, è denominato "gestore dei servizi telematici"[15].

In altre parole, l'insieme delle macchine e dei programmi, con i quali il Ministero della Giustizia tratta i procedimenti e interagisce con l'esterno ricevendo depositi e pagamenti o inviando comunicazioni e notificazioni di cancelleria, è definito dall'art. 1, lett. a, d.m. 44/2011 come il "Dominio Giustizia". Dal suo interno operano i soggetti abilitati interni (giudici, cancellieri e ufficiali giudiziari), dall'esterno, invece, tutti gli altri soggetti, i c.d. abilitati esterni (avvocati, consulenti di ufficio, ecc., utenti privati). All'interno del Dominio Giustizia vi sono i registri informatizzati di cancelleria che contengono a loro volta i singoli fascicoli informatici di ciascuna causa o procedura giudiziaria[16].

---

tradizionalmente intercorrenti tra i soggetti del processo – siano essi c.d. "soggetti abilitati esterni" al sistema informatico, cioè difensori o esperti ed ausiliari del giudice, o c.d. "soggetti abilitati interni", cioè magistrati, personale di cancelleria o degli Unep – e tra essi e l'ufficio giudiziario, nell'ambito del processo civile».

[14] Da https://www.csm.it/web/csm-internet/il-processo-civile-telematico/legenda?redirect=/web/csm-internet/il-processo-civile-telematico/legenda&show=true&title=le%20definizioni%20del%20PCT&show_bcrumb=le%20definizioni%20del%20PCT «l'insieme delle risorse hardware e software, mediante il quale il Ministero della giustizia tratta in via informatica e telematica qualsiasi tipo di attività, di dato, di servizio, di comunicazione e di procedura».

[15] https://www.csm.it/web/csm-internet/il-processo-civile-telematico/legenda?redirect=/web/csm-internet/il-processo-civile-telematico/legenda&show=true&title=le%20definizioni%20del%20PCT&show_bcrumb=le%20definizioni%20del%20PCT «sistema informatico, interno al dominio giustizia, che consente l'interoperabilità tra i sistemi informatici utilizzati dai soggetti abilitati interni, il portale dei servizi telematici e il gestore di posta elettronica certificata del Ministero della giustizia».

[16] L'architettura del PCT è basata su determinati sistemi per la gestione dei flussi che entrano ed escono dal Dominio Giustizia, fra i quali ci sono l'infrastruttura PEC (ovvero il Gestore di PEC Giustizia) – essa è composta dai gestori di PEC del Ministero della Giustizia sotto vigilanza di Agid. I singoli uffici dei vari distretti SICI si dotano di caselle PEC dedicate alla gestione dei flussi telematici in entrata e in uscita dal Dominio Giustizia –, il portale dei servizi telematici (PST) – ovvero il sistema centrale, previsto dall'art. 6 del d.m.44/2011 e succ. modifiche e dagli artt. 5 e 6 delle Specifiche Tecniche di cui al Provv. Resp. DGSIA 16 aprile 2014, che eroga a professionisti e cittadini i servizi di consultazione e pagamento telematico e che gestisce i servizi centralizzati quali principalmente il Registro Generale degli Indirizzi Elettronici, il sistema di Verifica Certificati e la conservazione del log della PEC. Rende disponibile i servizi del dominio Giustizia per l'accesso dall'esterno di magistrati, software house, Punti di Accesso (che sono punti di accesso ai registri gestiti da privati o da ordini professionali) mediante autenticazione forte basata su smart-card –,il ReGIndE – ovvero il

Il Dominio giustizia comunica all'esterno attraverso la descritta infrastruttura generando dei flussi, i quali possono essere catalogati in: consultazioni dei registri di cancelleria[17], pagamenti telematici[18], depositi[19] dei

Registro Generale degli Indirizzi Elettronici (ReGIndE) gestito dal Ministero della giustizia e previsto dall'art. 7 del d.m. 44/2011 e succ. modifiche e dagli artt. 7, 8 ed 9 delle Specifiche tecniche di cui al Provv. Resp. DGSIA 16 aprile 2014. Questo è il registro nel quale sono riportati gli indirizzi PEC di tutti i soggetti esterni abilitati ai depositi nei registri di cancelleria. Se l'indirizzo PEC non è stato preventivamente comunicato al Reginde (per gli avvocati vi provvede il Consiglio dell'Ordine di appartenenza) l'abilitato esterno non può effettuare depositi e non può ricevere comunicazioni/notificazioni di cancelleria –, ed, infine, il citato gestore dei servizi telematici, composto da Gestore Locale (GL) – che implementa l'insieme di tutti i servizi applicativi esposti dagli Uffici Giudiziari di un distretto con riguardo al Processo Civile Telematico. Le tipologie di servizi telematici sono: - gestione delle fasi di ricezione, controllo e accettazione dell'atto di parte; - l'interfacciamento con il Repository Documentale; - invio degli esiti automatici e quello a seguito dell'accettazione del deposito; - invio atti all'esterno ovvero comunicazioni/notificazioni telematiche; - pagamenti telematici: effettua la verifica della ricevuta collegandosi al PST e controllando l'identificativo univoco del pagamento; - configurazione dei servizi di interrogazione verso la base dati dei sistemi di cancelleria a beneficio dei punti di accesso e delle software house che utilizzano i proxy di consultazione sul PST – e dal Gestore Locale della PEC – ovvero il modulo applicativo incaricato di interfacciare il gestore locale (GL) con il Gestore di PEC sub a) attraverso un flusso di lavoro specifico per la gestione dell'invio e della ricezione dei messaggi e delle ricevute di posta elettronica certificata.

[17] Attraverso il PST è possibile la consultazione da parte dei soggetti abilitati esterni e degli utenti privati dei registri di cancelleria. L'accesso è consentito anche senza autenticazione (c.d. accesso anonimo) ma in questo caso è esclusa la visibilità dei dati relativi ai nominativi delle parti e degli atti e dei provvedimenti archiviati all'interno del singolo fascicolo. Solo con l'accesso previa autenticazione (*login*), gli avvocati costituiti e gli ausiliari del giudice nominati in quel giudizio hanno accesso da remoto a queste altri dati. L'accesso anonimo, oltre che via internet sul Portale dei Servizi Telematici, è consentito anche tramite un'applicazione (Giustizia Civile) per la telefonia mobile predisposta dal Ministero della Giustizia.

[18] Attraverso il Portale dei Servizi Telematici è possibile per gli avvocati, previa autenticazione, accedere al servizio di pagamento telematico dei Contributo Unificato/Diritti di cancelleria o Diritti di Copia. Il sistema consente il pagamento attraverso diversi canali predisposti da banche e da Poste Italiane, le cui condizioni economiche sono pubblicizzate sul portale. Al termine della procedura di pagamento il sistema genera una ricevuta telematica (RT) che può essere salvata o stampata in formato PDF oppure salvata in formato elettronico .xml firmato da inserire successivamente nella busta di un deposito telematico.

[19] Come noto, il deposito è lo strumento con il quale la parte provvede a iscrivere a ruolo un nuovo procedimento, ossia a creare il contatto presso un ufficio giudiziario, oppure con il quale uno dei soggetti del procedimento provvede a far acquisire un certo atto al procedimento stesso, rendendone possibile l'inserimento nel fascicolo. Scopo del deposito di un atto è, poi, anche quello di mettere tale atto a disposizione del giudice e delle altre parti, rendendolo conoscibile (Per tutti, A. BONAFINE, *L'atto processuale telematico*, Napoli, 2017, 115 ss.; ma anche N. SOTGIU, *Il deposito telematico*, in G. RUFFINI (a cura di), *Il processo telematico nel sistema del diritto processuale civile*, cit., 226 ss.)

In conseguenza dell'introduzione delle disposizioni del processo telematico, il deposito si compie, senza accesso fisico presso la cancelleria, bensì in forma dematerializzata, mediante la trasmissione telematica di un atto o di un documento probatorio in formato elettronico. Tale forma, inizialmente prevista come obbligatoria solo per i depositi delle parti processuali successivi alla costituzione in giudizio (sovente indicati anche nella prassi come depositi endoprocessuali) e solo dinanzi a certi uffici giudiziari (cfr. art. 16 *bis* d.l. n. 179/2012, abrogato dal d.lg. n. 149/2022), è stata generalizzata per tutti i procedimenti, pressoché per tutti i soggetti del processo e per tutti gli atti, anche quando coincidenti con la presa di contatto con l'ufficio giudiziario (iscrizione a ruolo e costituzione delle parti). Tale generalizzazione risulta dagli artt. 196 *quater*-196 *sexies* disp. att. c.p.c., introdotti dall'art. 4, co. 12, d.lg. n. 149/2022 e destinati ad applicarsi anche ai procedimenti già pendenti alla data del 1° gennaio 2023 davanti al tribunale, alla corte di appello e alla Corte di cassazione (ed applicabili dinanzi agli uffici del giudice di pace dal 30 giugno 2023, sia per i procedimenti di nuova instaurazione sia per quelli già pendenti a tale data).

La logica del deposito telematico e della sua progressiva obbligatorietà ed esclusività risiede non tanto in esigenze di tipo organizzativo (risparmio di carta e di spazio occupato da volumi fisici, migliore gestione dei fascicoli e del lavoro di cancelleria), quanto piuttosto nel rendere disponibili in tempo reale (o comunque in un tempo ragionevolmente breve) gli atti, i provvedimenti e i documenti probatori in un fascicolo dematerializzato (il fascicolo informatico), accessibile a distanza con collegamento telematico, rendendo tali atti, documenti e provvedimenti conoscibili e più agevolmente fruibili ai soggetti del processo. Essa è, cioè, una forma funzionale all'esercizio del contraddittorio e del diritto di difesa nonché indispensabile allo scopo del processo telematico (N. SOTGIU, *Il deposito telematico*, cit., 226 ss.).

soggetti abilitati esterni e comunicazioni/notificazioni di cancelleria[20].

In riferimento alle notifiche, con il d.lg. n. 149/2022 sono state introdotte determinate notifiche che sia l'avvocato sia l'ufficiale giudiziario devono eseguire la forma telematica. In particolare, il legislatore ha previsto che, al ricorrere di determinati presupposti e nei confronti di certi destinatari, le notificazioni nell'interesse di una parte rappresentata da un difensore devono essere eseguite dall'avvocato invece che dall'ufficiale giudiziario e devono avvenire in forma telematica, ai sensi degli artt. 3 *bis* e 3 *ter* l. n. 53/1994, con

---

Alla luce della disciplina attualmente in vigore, contenuta negli artt. 196 q*uater*-196 *septies* disp. att. c.p.c. e integrata da fonti secondarie (regole tecniche e specifiche tecniche del processo civile telematico), si compiono in forma telematica, sostitutiva di quella tradizionale, i depositi di: atti e documenti probatori (nativi digitali o in copia informatica, anche per immagine, attestata conforme all'originale ai sensi dell'art. 196 *novies* disp. att. c.p.c.) del difensore, del dipendente di cui si avvale la pubblica amministrazione per stare in giudizio, dei soggetti nominati dalle parti, del PM e dei soggetti nominati e delegati dall'autorità giudiziaria (art. 196 *quate*r, co. 1, disp. att. c.p.c.); atti del personale degli uffici giudiziari, degli UNEP, del cancelliere e del segretario dell'ufficio (art. 196 *quinquies*, co. 1 e 3, disp. att. c.p.c.).
Con riferimento ai verbali di udienza e ai provvedimenti del giudice non c'è una chiara ed univoca indicazione di obbligatorietà del deposito telematico. Da un lato, infatti, l'art. 196 *quater*, co. 2, disp. att. c.p.c. (nel testo appositamente sostituito dall'art. 35, co. 3, lett. b, d.l. n. 13/2023), con formula assertiva, indica quella telematica come forma ordinaria di deposito ("Il deposito dei provvedimenti del giudice e dei verbali di udienza ha luogo con modalità telematiche"). Dall'altro, però, l'art. 196 *quinquies* disp. att. c.p.c. – non coordinato con la modificata lettera dell'art. 196 *quater*, co. 2, disp. att. c.p.c. – sembra mantenere aperta la possibilità per i magistrati di redigere i provvedimenti in formato cartaceo e di eseguirne il deposito con materiale consegna presso la cancelleria, con obbligo in questo caso per il cancelliere di estrarre copia informatica e provvedere all'inserimento nel fascicolo informatico (sul punto, v. G. RUFFINI (a cura di), *Diritto processuale civile*, vol. I, *La giustizia civile*, cit., 243 ss., soprattutto per le ipotesi residuali di deposito in modalità tradizionale).
Con riferimento ai provvedimenti del giudice e ai verbali di udienza, la norma di riferimento è ancora l'art. 16 delle specifiche tecniche del 2014, in base alla quale essi vengono inseriti in una busta telematica trasmessa su canale sicuro al gestore dei servizi telematici del dominio giustizia.
Il deposito degli atti processuali e dei documenti probatori ad opera dei difensori delle parti avviene tuttora con la trasmissione di un messaggio di posta elettronica certificata, avente come oggetto la parola "deposito", dall'indirizzo PEC risultante dal ReGIndE all'indirizzo PEC dell'ufficio destinatario, secondo la disciplina del d.m. n. 44/2011 e delle specifiche tecniche del processo telematico. In allegato al messaggio PEC viene inviata una busta telematica, il cui contenuto è previsto dalle specifiche tecniche, secondo le quali l'atto depositato deve essere in forma di documento informatico, ossia nativo digitale, in formato .pdf, sottoscritto digitalmente o con firma elettronica qualificata e con i requisiti indicati dall'art. 12 delle specifiche tecniche.

[20] Comunicazioni e notificazioni, nel sistema originario del codice civile, avvenivano per lo più mediante operazioni di tipo materiale e con la consegna di biglietti e atti cartacei.
Il passaggio alla forma telematica, già anticipato e reso facoltativo per le comunicazioni dalla l. n. 183/2011, è avvenuto in modo più deciso, sia per le comunicazioni che per le notificazioni, con l'avvento del processo civile telematico (a partire dal d.l. n. 179/2012) (cfr. F. PORCELLI, *Le comunicazioni e le notificazioni*, in G. RUFFINI (a cura di), *Il processo telematico nel sistema del diritto processuale civile*, cit., 329 ss.).
Tecnicamente comunicazioni e notificazioni telematiche avvengono presso il domicilio digitale, risultante da pubblici elenchi[20]. La titolarità di un domicilio digitale risultante da pubblici elenchi è stata assunta dal legislatore come condizione in presenza della quale le comunicazioni e, per effetto del d.lg. n. 149/2022, le notificazioni debbono avvenire in via telematica. I pubblici elenchi richiamati dalle disposizioni relative alle comunicazioni e notificazioni telematiche sono quelli previsti nell'art. 16 *ter* d.l. n. 179/2012, consultabili telematicamente. Ferme le diverse nozioni e funzioni delle comunicazioni e delle notificazioni di cancelleria, la normativa del processo civile telematico disciplina le modalità di compimento delle une e delle altre in modo sostanzialmente unitario, con disposizioni contenute nell'art. 16 d.l. n. 179/2012 e successive modificazioni. In proposito la scelta operata dal legislatore con la norma citata è stata quella di stabilire per le comunicazioni (e notificazioni) di cancelleria la tendenziale esclusività della forma telematica, sia per alleggerire il lavoro delle cancellerie, sia per incentivare forme dematerializzate di compimento degli atti nella prospettiva del processo civile telematico. In questa stessa ottica, il legislatore ha inoltre previsto le conseguenze dell'impossibilità di eseguire tali atti in modalità telematica; mentre residuali risultano in tale sistema le modalità analogiche. In tema di notificazioni in via telematica, è rilevante la distinzione tra notifiche assoggettate alla disciplina successiva all'entrata in vigore del d.lg. n. 149/2022 e quelle assoggettate alla disciplina anteriore.

certe modalità[21]. Con riferimento alle notifiche di atti stragiudiziali e di atti processuali relativi a procedimenti instaurati dal 1° marzo 2023 e che l'ufficiale giudiziario è tenuto ad eseguire, è previsto dall'art. 149 *bis* c.p.c. (nel testo sostituito dall'art. 3, co. 11, lett. e, d.lg. n. 149/2022) che, quando il destinatario sia un soggetto tenuto per legge a munirsi di un indirizzo PEC o SERCQ oppure abbia volontariamente eletto domicilio digitale nell'INAD, le notifiche siano compiute in forma telematica (sempre a condizione che non debbano essere eseguite dall'avvocato e che gli uffici NEP siano dotati delle necessarie strumentazioni)[22].

1.2. La normativa secondaria.

In riferimento al quadro normativo secondario, occorre segnalare che da una parte vi sono le fonti regolamentari, che istituiscono le cc.dd. regole tecniche, dall'altra parte vi sono le specifiche tecniche, ovvero la concreta applicazione delle regole. Se le prime sono contenute in decreti ministeriali, le seconde spesso sono individuate da provvedimenti di appositi dipartimenti del Ministero stesso (tendenzialmente ascrivibile alla Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia).

Come si è potuto constatare dalla ricostruzione del tessuto normativo fondante il PCT e la sua applicazione al c.c.i., la maggior parte dei meccanismi legati al funzionamento dell'informatizzazione sono contenuti nel d.m. 21 febbraio 2011 n. 44 - pubblicato nella G.U. n° 89 del 18-04-2011, ovvero nel Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24. In particolare, emergono i provvedimenti legati alle specifiche tecniche di cui all'art. 34 del d.m. 21 febbraio 2011 n. 44 e alle disposizioni di cui all'art. 35 dello stesso: a tal proposito vi sono i decreti di attivazione degli indirizzi PEC degli uffici giudiziari e il Provvedimento 28 dicembre 2015 (modifiche alle specifiche tecniche *ex* art. 34 d.m. 44/2011). Vi sono inoltre i d.m. 27 Aprile 2009 (Nuove Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia) e d.m. 27 Marzo 2000 n. 264 (Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari).

Inoltre, da ultimo si segnala che a decorrere dal 22 agosto 2023, a norma dell'art. 155 *quater* disp. att. c.p.c., ultimo periodo, è stato predisposto l'accesso diretto da parte dell'ufficiale giudiziario, attraverso il Sistema di Interscambio

[21] Cfr. art. 137, co. 7, c.p.c. (nel testo sostituito dall'art. 3, co. 11, lett. b, d.lg. n. 149/2022), dall'art. 3 *ter* l. n. 53/1994 (introdotto dall'art. 12, co. 1, lett. b, d.lg. n. 149/2022) e dall'art. 4, co. 1, secondo periodo, l. n. 53/1994 (aggiunto dall'art. 12, co. 1, lett. c, d.lg. n. 149/2022), norme applicabili alle notificazioni di atti stragiudiziali compiute dal 28 febbraio 2023 e alle notificazioni di atti processuali riguardanti procedimenti instaurati a far data dal 1° marzo 2023

[22] Le modalità concrete con cui la notificazione si compie sono individuate dallo stesso art. 149 *bis* c.p.c., dall'art. 17 delle regole tecniche (di cui al d.m. n. 44/2011) e dall'art. 19 delle specifiche tecniche del processo civile telematico contenute nel provvedimento del Ministero della giustizia – d.g.s.i.a. del 16 aprile 2014, e successive modificazioni. Anche esse si articolano nella fase di impulso, nella quale viene presentata l'istanza all'ufficiale giudiziario, nella fase di trasmissione e in quella di documentazione.

flussi Dati (SID), alle banche dati dell'Agenzia delle Entrate quali la Dichiarazioni dei Redditi e Certificazione unica, gli atti del Registro e l'archivio dei Rapporti finanziari[23].

Procedimenti simili sono individuati anche per la normativa sulla PEC e sulla notifica telematica, dove si adotta sempre la tripartizione: norma di rango primario che individua il principio, norma regolamentare che ne disciplina il funzionamento, regola e specifica tecnica per i dettagli applicativi[24].

2. Il processo telematico nel Codice della crisi.

I temi del processo telematico e le relative procedure di automazione hanno toccato anche le procedure concorsuali. L'art. 360 c.c.i. ha disposto l'inserimento del comma 4 *bis* nell'art. 16 *bis* d.l. 179/2012 secondo cui nei procedimenti giudiziali volti all'apertura delle procedure concorsuali, in tutti i gradi del giudizio, gli atti processuali dei difensori o degli ausiliari del giudice e i relativi documenti devono essere obbligatoriamente depositati con modalità telematiche, nel rispetto della disciplina (anche) regolamentare dettata in materia di documento informatico e di PCT (e, dunque, di quanto disposto dal C.a.d. di cui al d.lg. 82/2005 e dalle regole e specifiche tecniche del processo civile telematico)[25]. L'introduzione di elementi di "informatizzazione" delle procedure concorsuali in realtà è assai più risalente, poiché alcune innovazioni erano state previste già in sede di modifica della vecchia legge fallimentare[26], ad esempio in materia di comunicazioni, richieste di iscrizione nel registro delle imprese da parte del cancelliere, decisioni del comitato dei creditori, adunanza dei creditori per esaminare lo stato passivo e per l'approvazione della proposta di concordato.

La legge delega per la riforma delle discipline della crisi di impresa e dell'insolvenza denota l'intento del delegante di realizzare, a regime, un notevole rafforzamento della dimensione telematica nell'ambito delle procedure concorsuali, lungo varie direttrici[27].

---

[23] https://pst.giustizia.it/PST/en/dettaglio_schede_tematiche.page?contentId=ACC2849&modelId=12.

[24] V. https://pst.giustizia.it/PST/resources/cms/documents/SpecificheTecnicheTestoCoordinatoArticolato.pdf.

[25] L'art. 360, inoltre, nel richiamare l'applicazione della disciplina del secondo periodo del comma 4 dell'art. 16 *bis* d.l. 179/2012, fa salvo il potere del Presidente del tribunale di autorizzare il deposito con modalità non telematiche (il che evidentemente può significare consegna/trasmissione degli atti in forma cartacea, *brevi manu* o a mezzo posta, o anche mediante consegna diretta di supporti informatici, come dvd/cd-rom) allorché i sistemi informatici ministeriali non siano funzionanti e sussista una indifferibile urgenza, così riproponendo l'eccezione all'obbligo di deposito telematico degli atti espressamente prevista nel procedimento di ingiunzione. Benché non espressamente disciplinata, non può non considerarsi l'ipotesi in cui la necessità di depositare in cartaceo non derivi da disfunzioni delle infrastrutture informatiche, ma dall'impossibilità di depositare taluni atti o documenti in formato digitale per ragioni di formato o di dimensioni (si pensi ai file audio o video, non ammessi dalle specifiche tecniche del PCT o alla lastra di una radiografia): in questi casi dovrà essere il tribunale concorsuale (e non il capo dell'ufficio) ad autorizzare il deposito in modalità analogica per "ragioni specifiche" in forza dell'applicazione estensiva dell'art. 16 *bis*, comma 9, d.l. 179/2012.. In tal senso, G.G. Poli, *Le misure di informatizzazione delle procedure della crisi e dell'insolvenza*, cit., 119.

[26] Cfr. d.lg. 169/2007.

[27] A. Bonafine, *L'atto processuale telematico*, cit., 115 ss.; G. Bonfante, *Il nuovo diritto della crisi e dell'insolvenza*, in *Giur. it.*, 2019, 1943 ss.; L. De Simone, *La gestione del processo telematico nelle procedure*

A ciò può aggiungersi che la c.d. direttiva *insolvency* (UE 2019/1023) del Parlamento europeo e del Consiglio del 20 giugno 2019 ha prescritto agli Stati membri, tra le misure volte a favorire l'efficienza delle procedure, l'adozione di disposizioni che consentano alle parti coinvolte nelle procedure, ai professionisti e alle autorità giudiziarie l'utilizzo dei mezzi di comunicazione informatica almeno per alcune attività tassativamente indicate (tra cui si segnalano le insinuazioni al passivo, la presentazione di piani di ristrutturazione e rimborso, le notifiche ai creditori, la presentazione di impugnazioni e contestazioni).

Il quadro di principi citato ha indotto parte della dottrina ad affermare che «il Codice della Crisi abbia, pur con diverse stratificazioni dovute ai plurimi interventi correttivi, adempiuto (almeno formalmente) ai compiti impartiti dal legislatore delegante e alle indicazioni pro- venienti dagli organi dell'Unione, attraverso una serie di disposizioni di stampo innovativo rispetto al tessuto della legge fallimentare, finalizzate a rafforzare la dimensione telematica delle procedure»[28].

D'altra parte, l'obbligo di deposito digitale oggi imposto dal c.c.i. ai difensori o ausiliari del giudice in relazione a tutti gli atti e documenti processuali (siano essi atti introduttivi e di costituzione in giudizio ovvero endoprocessuali e quindi successivi alla costituzione delle parti) sussiste già, in forza dell'art. 16 *bis*, comma 3, d.l. 179/2012, in capo agli organi delle procedure concorsuali, e segnatamente al curatore, commissario giudiziale, liquidatore, commissario liquidatore e commissario straordinario, in relazione ad atti interni alle suddette procedure[29].

---

concorsuali, in *Fallimento*, 2020, 1476; F. FERRARI, *Il deposito telematico della domanda di fallimento*, in *Giur. comm.*, 2015, 1340; G. FICHERA, *La transizione verso il codice della crisi: ancora molte norme da attuare*, in *www.altalex.com*; M. GABOARDI, *Spunti sulla legge delega per la riforma organica delle procedure concorsuali: profili processuali*, in *Riv. società*, 2019, 123 ss.; F. VALERINI, *Pubblicato il decreto dirigenziale sulla composizione negoziata della crisi di impresa*, in www.ilfallimentarista.it.

Su un piano generale, il criterio posto dall'art. 2, comma 1, lett. h della l. 19 ottobre 2017, n. 155 ha affidato all'Esecutivo il compito di "uniformare e semplificare, in raccordo con le disposizioni sul processo civile telematico, la disciplina dei diversi riti speciali previsti dalle disposizioni in materia concorsuale". In secondo luogo, sempre in un'ottica trasversale a tutti i procedimenti volti alla regolazione della crisi e dell'insolvenza, la lett. i del richiamato art. 2 l. 155/2017 ha incaricato il Governo di prevedere che la notificazione nei confronti del debitore (professionista o imprenditore) degli atti delle procedure concorsuali e, in particolare, dell'atto iniziale del procedimento finalizzato all'accertamento dello stato di crisi dovesse eseguirsi obbligatoriamente presso l'indirizzo del servizio elettronico di recapito certificato qualificato o presso l'indirizzo PEC del debitore risultante da elenchi pubblici, nonché di disciplinare (in subordine) le modalità della procedura telematica alternativa per l'effettuazione della notifica, quando questa si fosse rivelata impossibile o non fosse andata a buon fine, per causa imputabile al destinatario. A questo fine la legge delega ha anche previsto che nei decreti attuativi si imponesse all'imprenditore di mantenere attivo il proprio domicilio digitale (servizio di recapito elettronico o PEC) fino all'anno successivo alla cancellazione dal registro delle imprese. Sul tema, cfr. G.G. POLI, *Le misure di informatizzazione delle procedure della crisi e dell'insolvenza*, in G. TRISORIO LIUZZI (a cura di), *Diritto della crisi d'impresa*, Bari, 2023, 118: «Appare evidente, poi, come tutti questi specifici criteri di delega potessero ricondursi alla generale direttiva (v. art. 2, comma 1, lett. l della l. 155/2017) di contenimento della durata e dei costi complessivi delle procedure concorsuali, perseguibile attraverso la dematerializzazione di atti ed attività tipica del processo civile telematico».

Inoltre, limitatamente al procedimento di liquidazione giudiziale, l'art. 7, comma 8, della legge delega ha previsto, ai fini del perseguimento degli obiettivi di maggiore rapidità, snellezza e concentrazione dell'accertamento del passivo, l'adozione di misure volte ad agevolare la presentazione in via telematica delle domande di insinuazione da parte di creditori e terzi, anche se residenti all'estero

[28] G.G. POLI, *Le misure di informatizzazione delle procedure della crisi e dell'insolvenza*, cit., 118.

[29] Osserva G.G. POLI, *Le misure di informatizzazione delle procedure della crisi e dell'insolvenza*, cit., 120: «Nulla ha previsto il legislatore della riforma (in linea con il silenzio serbato dalla disciplina generale del deposito

Con riferimento alla necessità di prevedere forme telematiche di notificazione al debitore degli atti delle procedure concorsuali (e in particolare dell'atto introduttivo del procedimento per l'accertamento dello stato di crisi), la delega si è tradotta nei commi 6, 7 e 8 dell'art. 40 c.c.i. che disciplinano, in via gradata, le tre diverse modalità per informare il debitore dell'avvio nei suoi confronti di un procedimento di regolazione della crisi e dell'insolvenza o della liquidazione giudiziale.

In primo luogo si prevede che, in caso di proposizione della domanda introduttiva del procedimento unitario (per l'accesso agli strumenti di regolazione della crisi o dell'insolvenza e alla liquidazione giudiziale) da parte di soggetti diversi dal debitore stesso (creditore, pubblico ministero, organo di controllo interno, autorità che hanno poteri di vigilanza o controllo sull'impresa), il ricorso e il decreto di convocazione emesso dal tribunale debbano essere notificati al debitore, a cura dell'ufficio, alternativamente presso l'indirizzo risultante dal servizio elettronico di recapito certificato qualificato o all'indirizzo di posta elettronica certificata del debitore, risultante dal registro delle imprese o dall'INI-PEC e che l'esito della comunicazione venga trasmesso per via telematica all'indirizzo PEC del ricorrente. Subordinatamente, quando cioè la notificazione presso il domicilio digitale del debitore sia risultata impossibile o non abbia sortito esito positivo per causa imputabile al destinatario, la notificazione dovrà essere effettuata senza indugio, a cura della cancelleria, mediante inserimento del ricorso e del decreto nell'area web riservata disciplinata dall'articolo 359 c.c.i.. Secondo uno schema *lato sensu* sanzionatorio a carico del debitore, la conoscenza legale della notifica da parte del destinatario è qui ricollegata al mero decorso di un termine (del terzo giorno successivo a quello in cui è stato effettuato l'inserimento) a prescindere dalla conoscenza effettiva (pur se il debitore dovrà essere informato dell'avvenuto inserimento dell'atto).

Secondo il richiamato art. 359[30], l'area web riservata in parola è realizzata dal Ministero dello sviluppo economico (sentita l'Agenzia per l'Italia digitale) avvalendosi delle strutture informatiche in uso presso le camere di commercio, previa emanazione di un decreto chiamato a disciplinare alcuni aspetti cruciali, tra cui: la codifica degli eventi che generano avvisi di mancata consegna, distinguendo tra quelli imputabili e quelli non imputabili al destinatario; le modalità di inserimento automatico degli atti nell'area web riservata; le modalità di accesso a ciascuna area da parte dei rispettivi titolari; le modalità di comunicazione al titolare dell'area web riservata del link per accedere agevolmente all'atto oggetto della notifica, escludendo la rilevanza di questa comunicazione ai fini del perfezionamento della notifica, già avvenuta per effetto dell'inserimento di cui alla lettera seguente; il contenuto e le modalità di rilascio alla cancelleria dell'attestazione dell'avvenuto inserimento dell'atto da notificare nell'area web riservata; il contenuto della ricevuta di avvenuta notifica mediante inserimento nell'area web riservata e le modalità di firma

telematico degli atti nel processo civile, di cui all'art. 16-*bis* d.l. 179/2012) circa le conseguenze processuali dell'eventuale inosservanza dell'obbligo di deposito telematico», prospettando il perpetuarsi di dispute, in giurisprudenza e dottrina, circa i possibili esiti.

[30] A. TEDOLDI, *art. 359 CCII*, in A. MAFFEI ALBERTI (diretto da), *Commentario breve alle leggi su crisi d'impresa ed insolvenza*, 7ª ed., Milano, 2023, 2580 ss.

elettronica; il periodo di tempo per il quale è assicurata la conservazione dell'atto notificato nell'area web riservata; le misure necessarie ad assicurare la protezione dei dati personali[31].

Occorre segnalare, però, che con l'art. 4 *ter* del d.l. n. 51/2023 come convertito dalla l. n. 87 del 3 luglio 2023 (pubblicata nella Gazzetta Ufficiale del 5 luglio 2023), il Legislatore ha sospeso fino al 31 dicembre 2023 l'efficacia dei nuovi commi 2 e 3 dell'art. 3 *ter* della l. 53/94 introdotto dal d.lg. n. 149/22 entrato in vigore il 1° marzo 2023.

Fatta salva la sostituzione del meccanismo di deposito fisico con quello di inserimento digitale nell'istituenda area web, l'assetto ricalca quello dettato dall'art. 16, comma 6, d.l. 179/2012 con riguardo alle comunicazioni e notificazioni di cancelleria nei procedimenti civili, alla cui stregua "Le notificazioni e comunicazioni ai soggetti per i quali la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata, che non hanno provveduto ad istituire o comunicare il predetto indirizzo, sono eseguite esclusivamente mediante deposito in cancelleria. Le stesse modalità si adottano nelle ipotesi di mancata consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario".

In ulteriore ed estremo subordine, quando l'impossibilità della notificazione o l'esito infausto della stessa siano dipesi da una causa non addebitabile al destinatario (o in via transitoria, ma solo fino alla realizzazione della suddetta area web, anche nelle ipotesi in cui tali eventi risultino imputabili al destinatario), sarà ammesso il ricorso alle forme tradizionali di notifica.

Riepilogando, l'articolata disciplina della notificazione nei confronti del debitore degli atti introduttivi (ricorso e decreto) del procedimento unitario per l'accesso agli strumenti di regolazione della crisi e dell'insolvenza e alla liquidazione giudiziale si snoda secondo modalità gerarchicamente ordinate, che prevedono: a) la notificazione, a cura della cancelleria, presso il domicilio digitale del debitore; b) in caso di notifica non eseguibile con le modalità *sub* a) per causa imputabile al destinatario, l'inserimento dell'atto a cura della cancelleria in uno spazio virtuale riservato al debitore, allo stato non ancora realizzato dal ministero competente; c) in caso di impossibilità o mancata consegna della notifica secondo le modalità *sub* a) per eventi non imputabili al destinatario (e, transitoriamente, anche in caso di eventi imputabili al destinatario), la notifica, a cura del ricorrente, nelle forme tradizionali e segnatamente c1) di persona, a mezzo ufficiale giudiziario, presso la sede dell'impresa o, per i soggetti non iscritti al registro delle imprese, presso la loro residenza; ovvero c2) quando le modalità di cui alla c1) non siano attuabili (per irreperibilità del destinatario), mediante il deposito dell'atto nella casa comunale del destinatario, con simultaneo perfezionamento della notifica e necessità di rendere edotti del deposito dell'atto i soli destinatari (persone fisiche) non tenuti dalla legge a dotarsi di un domicilio digitale.

[31] G.G. Poli, *Le misure di informatizzazione delle procedure della crisi e dell'insolvenza*, cit., 123 afferma che «gli aspetti che dovranno essere disciplinati nel suddetto decreto del M.I.S.E. non si limitano a quelli squisitamente tecnico-informatici, ma riguarderanno anche controverse questioni giuridiche, se si pensa in particolare alla distinzione tra eventi imputabili e non imputabili al destinatario, essenziale per determinare il ricorso a differenti modalità di notificazione: il che non può non suscitare serie perplessità a causa dell'affidamento ad una fonte secondaria di scelte in grado di incidere sensibilmente sul processo (e sul contraddittorio) e che, in quanto tali, devono trovare la loro disciplina nella legge (v. art. 111 Cost)».

In linea con il principio della velocizzazione delle procedure e della digitalizzazione dei flussi informativi, da attuarsi (oltre che per gli atti introduttivi) anche per quelli successivi e interni alle procedure concorsuali (v. art. 2, comma 1, lett. i, l. 155/2017), l'art. 10 c.c.i. ha previsto che tutte le comunicazioni effettuate dagli organi di gestione, controllo, assistenza (ad es. dal curatore nella liquidazione giudiziale)[32] siano eseguite esclusivamente per via telematica presso l'indirizzo PEC o il recapito elettronico certificato qualificato del destinatario (c.d. «domicilio digitale» ai sensi dell'art. 1 lett. n *ter* d.lg. 82/2005). A tal fine, il comma 2 dell'art. 10[33] prevede che i suddetti organi di gestione, controllo o assistenza delle procedure siano tenuti ad attivare un domicilio digitale, dandone tempestiva comunicazione agli interessati, da utilizzare per le comunicazioni inerenti alla procedura, in particolare ai creditori e titolari di diritti sui beni che non abbiano obbligo di munirsene, ai soggetti con sede o residenza all'estero e ai debitori e al legale rappresentante della società sottoposta ad una delle procedure disciplinate dal c.c.i.. Le spese per l'attivazione del domicilio digitale a favore di questi soggetti[34] sono poste a carico della massa. In caso di impossibilità di eseguire o di mancata consegna della comunicazione telematica per causa imputabile al destinatario – ipotesi partitamente riconducibili, ai sensi del comma 3 dell'art. 10, alla mancata attivazione o comunicazione agli organismi competenti del domicilio digitale ovvero ad una non corretta vigilanza sul corretto funzionamento della casella PEC (saturazione, presenza di virus) – essa si perfezionerà mediante semplice deposito dell'atto in cancelleria, senza necessità di compiere ulteriori formalità da parte della stessa. Dovranno osservarsi, poi, analoghe modalità di comunicazione da parte della cancelleria nei confronti dei soggetti a cui è stato assegnato d'ufficio un domicilio digitale, nel caso in cui la mancata consegna della comunicazione telematica sia riferibile ad una causa imputabile al destinatario[35].

Un altro importante risultato delle applicazioni ICT riguarda l'istruttoria sui debiti risultanti dai pubblici registri nei procedimenti per l'apertura della liquidazione giudiziale o del concordato preventivo. Infatti, l'art. 42 [36], in combinato disposto con l'art. 367 c.c.i.[37], introduce meccanismi di accesso alle informazioni riguardanti il debitore nelle procedure di liquidazione giudiziale e concordato preventivo mediante consultazione delle banche dati pubbliche in via telematica.

---

[32] V. art. 128 c.c.i..

[33] L'art. 38 d.l. 24 febbraio 2023, n. 13, ha rinviato di 18 mesi l'attivazione d'ufficio.

[34] A seguito del recepimento di una osservazione formulata nel parere del Consiglio di Stato n. 2854/2018 sullo schema dell'originario decreto legislativo di riforma del Codice della crisi e dell'insolvenza.

[35] Cfr. G.G. POLI, *Le misure di informatizzazione delle procedure della crisi e dell'insolvenza*, cit., 127, il quale aggiunge che «La legge nulla dice in ordine alla evenienza in cui la comunicazione per via telematica non sia stata resa possibile o non sia andata a buon fine per causa non imputabile al destinatario (mancata attivazione tempestiva, da parte dell'ufficio, del domicilio digitale in capo ad un soggetto non tenuto a dotarsene per legge o malfunzionamenti del sistema informatico dell'ufficio giudiziario mittente), ma va da sé che in tal caso debba trovare applicazione la disciplina prevista, in via generale, dall'art. 16, comma 8, d.l. 179/2012 secondo cui la cancelleria dovrà provvedere alla comunicazione a mezzo fax o consegna all'ufficiale giudiziario per la notifica nei confronti del destinatario».

[36] Cfr. A. ZACCARIA e M. FACCIOLI, *art. 42 CCII*, in A. MAFFEI ALBERTI (diretto da), *Commentario breve alle leggi su crisi d'impresa ed insolvenza*, 7ª ed., Milano, 2023, 265 ss.

[37] V. A. TEDOLDI, *art. 367 CCII*, in A. MAFFEI ALBERTI (diretto da), *Commentario breve alle leggi su crisi d'impresa ed insolvenza*, 7ª ed., Milano, 2023, 2587 ss.

Il meccanismo è forgiato su quello dettato dal codice di rito con riguardo alla ricerca telematica dei beni da pignorare (v. artt. 492 *bis* e ss. c.p.c. nonché artt. 155 *bis* e ss. disposizioni di attuazione c.p.c.) e prevede, come in quel contesto, differenti modalità di accesso ai dati rilevanti, ordinate in gradazione gerarchica discendente[38].

In primo luogo, si prevede (v. art. 42, co. 1) che, al di fuori delle ipotesi in cui la domanda di accesso alle procedure di insolvenza sia stata proposta dal debitore[39], la cancelleria acquisisce, mediante collegamento telematico diretto alle banche dati informatiche dell'Agenzia dell'entrate, dell'INPS e del Registro delle imprese i dati relativi al debitore indicati dall'art. 367, ove si prevede, nel dettaglio, che le pubbliche amministrazioni che gestiscono le banche dati dei tre soggetti testé indicati trasmettono automaticamente e direttamente alla cancelleria i dati indicati nei commi 2, 3 e 4 della disposizione e rispettivamente: il Registro delle imprese, i bilanci relativi agli ultimi tre esercizi, la visura storica, gli atti con cui sono state compiute le operazioni straordinarie e in particolare aumento e riduzione di capitale, fusione e scissione, trasferimenti di azienda o di rami di azienda; l'Agenzia delle entrate, le dichiarazioni dei redditi concernenti i tre esercizi o anni precedenti, l'elenco degli atti sottoposti a imposta di registro e i debiti fiscali, indicando partitamente per questi ultimi interessi, sanzioni e gli anni in cui i debiti sono sorti; l'Inps, le informazioni relative ai debiti contributivi.

Tuttavia, l'utilizzabilità informatica dei dati da parte delle cancellerie del tribunale della crisi potrebbe essere assicurata grazie alla stipula di singole convenzioni tra Ministero e enti pubblici gestori delle banche dati, onde consentire la consultazione a titolo gratuito e senza oneri per la finanza pubblica, come in qualche caso è stato già assicurato[40]. In ogni caso, sono state emanate le Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni in base alla lettera b comma 3 *ter* articolo 73 del d. lg. 7 marzo 2005, n. 82, da parte dell'Agenzia per l'Italia digitale, il 19 maggio 2023, per la conservazione e lo scambio di dati tra le pubbliche amministrazioni, anche se le stesse entreranno definitivamente operative quando le pubbliche amministrazioni che detengono i dati rilevanti non dispongano dei sistemi informatici per la cooperazione applicativa prevista dal codice dell'amministrazione digitale[41].

L'efficacia dell'art. 367 è soggetta al decorso del sessantesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale del provvedimento del responsabile dei sistemi informativi automatizzati del Ministero della giustizia, attestante la piena funzionalità del collegamento telematico, anche a seguito della stipula delle convenzioni di cui al comma 5, da adottarsi entro un anno dall'entrata in vigore del Codice (ovvero entro e non oltre il 15 luglio 2023).

Sono riconosciute prerogative simili a quelle concesse alla cancelleria ai fini dell'istruttoria preliminare nell'ambito dei procedimenti di concordato

[38] Sul punto, G.G. Poli, *Le misure di informatizzazione delle procedure della crisi e dell'insolvenza*, cit., 129.
[39] Sul quale grava un obbligo di produzione documentale nei termini specificati dall'art. 39.
[40] E v., da ultimo, la comunicazione del Dipartimento per la transizione digitale della giustizia, l'analisi statistica e le politiche di coesione del Ministero della Giustizia avente ad oggetto Banche dati di merito - Obiettivo P.N.R.R. M1-C1 Riforma 1.8 – Apertura agli utenti.
[41] Cfr. https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf.

preventivo e liquidazione giudiziale all'esperto, il quale è nominato da una commissione istituita presso le Camere di commercio di ciascun capoluogo di regione, nell'ambito della procedura di composizione negoziata per la soluzione della crisi d'impresa, su istanza dell'imprenditore che si trovi in condizioni di squilibrio patrimoniale o economico-finanziario che ne rendano probabile la crisi o l'insolvenza, quando risulti ragionevolmente perseguibile il risanamento dell'impresa.

L'accesso ai dati relativi alla situazione patrimoniale e debitoria dell'imprenditore è consentito all'esperto attraverso meccanismi di scambio di dati tra la piattaforma telematica nazionale[42] istituita ai sensi dell'art. 13 c.c.i. (e già operativa in forza di un decreto dirigenziale del Ministero della Giustizia emesso in data 28 settembre 2021) – cui ha accesso lo stesso imprenditore, i creditori che caricano i documenti (se prestano il consenso) e naturalmente l'esperto designato – e le banche dati dell'Agenzia delle entrate, dell'INPS, del Registro delle imprese, nonché le informazioni risultanti dalla centrale rischi presso la Banca d'Italia, con l'obiettivo di permettere all'esperto di testare l'esistenza di concrete prospettive di risanamento e avviare o proseguire le trattative con i creditori e con eventuali altri interessati.

Si segnalano, rispetto all'innovazione digitale del c.c.i., anche gli altri servizi offerti dalla piattaforma telematica nazionale, oltre a quelli in tema di composizione negoziata della crisi (cfr. artt. 12, 13, 14, 15, 17, 18 e 25 c.c.i.)[43] e di istituzione del programma informatico di verifica della sostenibilità del debito e di elaborazione di piani di rateizzazione (v. art. 25 *undecies* c.c.i.), vi è l'accesso alle banche dati da parte del cancelliere in fase istruttoria (art. 42 c.c.i.) e poi del curatore (art. 49, comma 3, lett. f, c.c.i.), nonché l'art. 367 c.c.i. sugli obblighi dei gestori di banche dati pubbliche.

Inoltre, il quadro è arricchito da una serie di disposizioni disseminate nel c.c.i. che riguardano la preferenza per le udienze, le adunanze e le operazioni di voto con modalità telematiche: cfr. art. 19 per il procedimento relativo alle misure protettive e cautelari; art. 107 per le modalità di voto telematico dei creditori nel concordato preventivo; art. 140 per le adunanze del Comitato dei creditori nella procedura di liquidazione giudiziale; art. 203 per l'adunanza per l'esame dello stato passivo. Anche in riferimento a comunicazioni e notificazioni, vi sono delle disposizioni che impongono l'utilizzo esclusivamente per via telematica di tali strumenti: cfr. art. 10, proprio sulle comunicazioni telematiche; ma v. anche, a titolo esemplificativo, le applicazioni degli artt. 40, 50, 51 spec. comma 6 in merito al procedimento unitario per l'accesso agli strumenti di regolazione della crisi e dell'insolvenza e alla liquidazione giudiziale, nonché il ruolo del domicilio digitale del curatore (art. 126); e, ancora, gli artt. 360 (sul deposito con modalità telematiche degli atti) e 361 (sul deposito telematico delle notifiche). L'orizzonte è completato dalla formazione della documentazione, come il mandato di pagamento sottoscritto dal giudice delegato e dal cancelliere con firma digitale e trasmesso telematicamente (cfr. art. 131,

[42] Già istituita con il d.l. 118/2021.

[43] Dove si regolamentano l'interoperabilità tra la piattaforma telematica nazionale per la composizione negoziata per la soluzione delle crisi d'impresa e le altre banche di dati; lo scambio di documentazione e di dati contenuti nella piattaforma telematica nazionale per la composizione negoziata per la soluzione delle crisi d'impresa tra l'imprenditore e i creditori; l'accesso alla procedura e il suo funzionamento tramite piattaforma telematica.

comma 4, c.c.i.), il registro informatico del curatore (art. 136)[44] e le modalità di liquidazione di cui all'art. 216.

La situazione testé delineata è, in realtà, costellata da qualche difficoltà applicativa, come testimoniato dai problemi riscontrati dalla Commissione Pagni, anche per il coordinamento con la riforma che ha introdotto il nuovo PCT: basti pensare all'iniziale assenza di convergenza tra le regole degli artt. 19 e 20 c.c.i. e il PCT[45], poi corretta con il d.lg. 83/2022.

3. Lo stato di attuazione.

Il livello di automazione che regola i flussi, di cui si è dato conto *supra*, passa necessariamente per tre tipologie di applicativi, due pubblici e uno privato: i primi due sono i registri di cancelleria e la consolle del magistrato; l'ultimo è il *software* in uso al professionista legale.

Partendo dai servizi erogati dal ministero in riferimento ai registri di cancelleria, i programmi, che assicurano le funzionalità del PCT, esistenti nelle cancellerie degli uffici giudiziari italiani per la gestione dei registri informatici per il contenzioso civile, volontaria giurisdizione, controversie di lavoro, esecuzioni, procedure concorsuali sono SICID e SIECIC.

SICID è l'acronimo di Sistema Informatico Contenzioso Civile Distrettuale e gestisce i registri del contenzioso civile, della volontaria giurisdizione e del contenzioso del lavoro ed è utilizzato nei tribunali e nelle corti di appello. Il manuale utente è scaricabile dal sito WikiAreaCivile della DGSIA, consultabile anche dall'esterno degli uffici giudiziari tramite le credenziali ADN.

SIECIC è l'acronimo di Sistema Informatico Esecuzioni Civili Individuali e Concorsuali e gestisce i registri delle esecuzioni e delle procedure fallimentari ed è presente solo nei tribunali.

I manuali utenti per le procedure esecutive individuali e per le procedure concorsuali sono scaricabili sempre dal sito WikiAreaCivile della DGSIA, consultabile anche dall'esterno degli uffici giudiziari con le credenziali ADN.

Per quanto riguarda la consolle del magistrato[46], essa è un'applicazione Java ed è l'unico programma che consente ai giudici ed ai suoi assistenti di gestire il PCT. Tramite questo programma il giudice, da un lato, ha la visione di tutto il suo ruolo e delle informazioni e dei dati di ciascuna procedura presenti nei registri di cancelleria, dall'altro, ha la possibilità di redigere, tramite Word di MS Windows, provvedimenti, di firmarli digitalmente e di trasmetterli al cancelliere per la loro pubblicazione all'interno del fascicolo informatico. La redazione è facilitata dalla possibilità di predisporre modelli di provvedimenti che, tramite l'inserimento dei c.d. *placeholders* o dei frasari, sfruttano per la loro

[44] Il comma 1 recita espressamente che il curatore "deve tenere un registro informatico, consultabile telematicamente, oltre che dal giudice delegato, da ciascuno dei componenti del comitato dei creditori e in cui deve annotare giorno per giorno le operazioni relative alla sua amministrazione. Mensilmente il curatore firma digitalmente il registro e vi appone la marca temporale, in conformità alle regole tecniche per la formazione, la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione dei documenti informatici".

[45] Sul punto, M. FABIANI, *La proposta della Commissione Pagni all'esame del Governo: valori, obiettivi, strumenti*, in *Diritto della crisi*, agosto 2021, passim.

[46] Sul punto, v. I. COPPOLA, *Consolle del Magistrato: Carneade chi era costui? Tra sistema di scrittura elettronica a banca dati di predictability. Qualche appunto*, in *questa rivista*, 2023, 1, 1 ss., spec. 5 ss.

compilazione i dati presenti nei registri.

Con la Consolle si possono fare ricerche giurisprudenziali ed esaminare i fascicoli messi in visione da altri giudici; il presidente della sezione può, inoltre, controfirmare i provvedimenti collegiali redatti dall'estensore.

Sono state di recente realizzate anche la Consolle di Udienza e la Consolle del PM (affari civili).

In particolare, le funzioni della Consolle del magistrato sono: la scrivania, l'agenda, le ricerche, il ruolo, il modellatore, la visualizzazione dei fascicoli, la redazione del provvedimento, gli appunti, la selezione di un report[47].

Per quanto riguarda il sistema di comunicazione tra il tribunale/cancelleria e l'avvocato, prima di descrivere il funzionamento dell'applicativo, occorre ricostruire, seppur brevemente, il sistema delle notificazioni telematiche dell'avvocato.

Nel sistema attualmente vigente occorre effettuare una distinzione, dal momento che coesistono due diversi regimi delle notificazioni telematiche a seconda che esse ricadano sotto la disciplina anteriore al d.lg. n. 149/2022 (destinata ad applicarsi ancora ad un vasto numero di casi e per diversi anni) oppure siano assoggettate alla disciplina introdotta dal citato d.lg.

In relazione ai giudizi già instaurati fino al 28 febbraio 2023 e sottoposti alla disciplina precedente al d.lg. n. 149/2022, la notifica telematica dell'avvocato al domicilio digitale del destinatario è facoltativa, nel senso che egli può scegliere, in alternativa, di richiedere la notificazione all'ufficiale giudiziario oppure di compierla in via analogica, nel rispetto dei requisiti e delle condizioni previste dalla l. n. 53/1994, o ancora di eseguirla telematicamente.

Inoltre, in caso di impossibilità o esito negativo della notificazione a mezzo PEC, indipendentemente dalla ragione di tale impossibilità o del mancato perfezionamento, gravava e tuttora grava sul notificante l'onere di riprendere l'iter notificatorio con le forme tradizionali e nei luoghi di cui agli artt. 137 ss. c.p.c. o ai sensi della l. n. 53/1994[48].

Con riferimento, invece, alle notifiche di atti processuali riguardanti procedimenti instaurati dal 1° marzo 2023 e per le notifiche di atti stragiudiziali dal 28 febbraio 2023, ai sensi dell'art. 137, co. 7, c.p.c. e dell'art. 3 *ter*, co. 1, l. n. 53/1994, non vi è alternatività tra la notifica dell'avvocato al domicilio digitale del destinatario e la notifica tradizionale. Infatti, ai sensi dell'art. 3 *ter*, co. 1, lett. a-b), l. n. 53/1994, il difensore munito di procura deve procedere alla notificazione telematica, mediante PEC (o, in prospettiva, mediante SERCQ) quando il destinatario sia un soggetto: tenuto a munirsi per legge di un

[47] Cfr. https://appellopct.files.wordpress.com/2012/11/manuale-consolle-del-magistrato.pdf.

[48] Rispetto a tale sistema, per le notifiche di atti riguardanti procedimenti già instaurati alla data del 28 febbraio 2023, costituisce eccezione la regola ricavabile dall'art. 16-*sexies* d.l. n. 179/2012, tuttora vigente, in combinato disposto con altre norme da esso implicitamente richiamate. In forza di tale disposizione, si può giungere alla notificazione dell'atto con il compimento di una semplice formalità, ossia con il deposito dell'atto in cancelleria, quando nel caso concreto ricorrono tutte le seguenti circostanze: a) trovano applicazione determinate disposizioni di legge le quali prevedono che il destinatario deve eleggere domicilio (fisico) nel luogo in cui ha sede il giudice davanti al quale pende il procedimento e stabiliscono che, in difetto di tale elezione, la notificazione può essere eseguita con deposito in cancelleria (cfr. ad esempio, art. 82 r.d. n. 37/1934, che onera l'avvocato che eserciti il patrocinio in un giudizio che si svolge fuori dalla circoscrizione territoriale cui è assegnato di eleggere domicilio nel luogo in cui si svolge il procedimento; art. 480, co. 3, c.p.c.); b) il destinatario non ha in concreto assolto l'onere di eleggere il domicilio ai sensi delle predette disposizioni; c) la notificazione telematica al domicilio digitale del destinatario risultante dai pubblici elenchi INI-PEC e RegGIndE non è possibile per causa a questi imputabile.

domicilio digitale risultante da pubblici elenchi (cioè un altro difensore, un professionista iscritto in albi o elenchi istituiti con legge dello Stato, una impresa in forma individuale o societaria, una pubblica amministrazione), ovvero, pur non essendo obbligato per legge a dotarsi di un domicilio digitale, ne abbia volontariamente istituito uno ai sensi dell'art. 3 *bis*, co. 1 *bis*, c.a.d. e tale domicilio risulti censito nel pubblico elenco INAD[49].

In accordo con quanto previsto dal d.m. n. 44 del 21 febbraio 2011 e dalle relative specifiche tecniche definite nel provvedimento del 16 aprile 2014, il deposito di un atto per via telematica è eseguito, come già ricordato, attraverso il sistema della PEC. L'atto e i suoi allegati devono essere inviati utilizzando un messaggio di PEC indirizzato all'ufficio giudiziario. Il professionista deve pertanto: essere censito nel Registro Generale degli Indirizzi Elettronici (RegIndE); essere dotato di casella di PEC, regolarmente censita nel RegIndE. Non possono essere utilizzate a tale scopo gli indirizzi di posta elettronica certificata per le comunicazioni tra cittadino e pubblica amministrazione (CEC-PAC); essere dotato di certificato di firma digitale su token crittografico (smart

[49] Per le conseguenze dell'impossibilità o del mancato perfezionamento della notifica al domicilio digitale di atti relativi a procedimenti instaurati dal 1° marzo 2023, v. G. Ruffini (a cura di), *Diritto processuale civile*, vol. I, *La giustizia civile*, cit., 232 ss. Venendo alle specifiche modalità di compimento delle notifiche eseguite dall'avvocato al domicilio digitale del destinatario, la disciplina attualmente esistente riguarda soltanto la notificazione mediante PEC e non anche quella da eseguirsi mediante il servizio elettronico di recapito certificato qualificato. La disciplina della notificazione mediante PEC prevede che: la notificazione deve avvenire esclusivamente utilizzando un indirizzo PEC del notificante risultante da pubblici elenchi, quale requisito indispensabile volto a consentire al destinatario di verificare l'attendibilità dell'indirizzo dal quale è stato trasmesso il messaggio PEC, prima di procedere alla sua apertura (art. 3 *bis*, co. 1, l. n. 53/1994); la notificazione si esegue trasmettendo l'atto a un indirizzo PEC risultante da pubblici elenchi, senza però che sia sancito l'esclusivo impiego di questi ultimi, con la conseguenza che – sia tenendo conto della funzione svolta dai pubblici elenchi, sia in base al principio di strumentalità delle forme – la notifica potrebbe essere legittimamente eseguita presso un domicilio digitale non censito in un pubblico elenco, al quale tuttavia il destinatario abbia dichiarato di voler ricevere le notificazioni relative al procedimento o che egli abbia indicato in atti; nell'oggetto del messaggio PEC deve essere indicata la dizione "Notificazione ai sensi della legge n. 53 del 1994" (art. 3 *bis*, co. 4), o altra dizione idonea a rendere consapevole il destinatario che si tratti di una notificazione e in assenza del quale può essere giustificata la mancata apertura del messaggio PEC. In allegato al messaggio PEC deve essere inserito l'atto notificando, che potrà essere: un atto nativo digitale, formato dal difensore (ad esempio, un atto di citazione da lui sottoscritto e non bisognoso di attestazioni di conformità); una copia informatica, anche per immagine, di un originale analogico in possesso del difensore e dichiarata conforme all'originale ai sensi dell'art. 3 *bis*, co. 2, l. n. 53/1994; oppure un duplicato o una copia informatica, anche per immagine, dichiarata conforme all'originale, ed estratta dal fascicolo informatico (art. 196 *octies* disp. att. c.p.c.); oppure ancora un atto misto. Al messaggio PEC deve essere, infine, allegata la relazione di notificazione, redatta dall'avvocato notificante su separato documento informatico e sottoscritta digitalmente, la quale deve recare i contenuti previsti dall'art. 3 *bis*, co. 5 e 6, l. n. 53/1994, fra i quali anche l'attestazione di conformità all'originale se l'atto notificato sia una copia informatica estratta dal difensore. La relata di notifica viene predisposta prima della trasmissione dell'atto, sicché se essa sicuramente è idonea a dare prova della volontarietà e della provenienza della notificazione, non è da sola sufficiente a provarne il compimento. A tale ultimo riguardo, rilevano le ricevute generate in fase di trasmissione e consegna relative al messaggio PEC. Queste sono la ricevuta di accettazione, generata dal gestore PEC del notificante, nel momento in cui ha avuto inizio la trasmissione e vi è stata la presa in carico del messaggio da parte del gestore PEC del mittente; e la ricevuta di avvenuta consegna, generata dal gestore PEC del destinatario, una volta che la trasmissione è stata completata e che il messaggio è stato recapitato nella casella PEC del destinatario. Ai sensi dell'art. 18, co. 6, d.m. n. 44/2011, la ricevuta di avvenuta consegna deve essere quella completa, ossia quella contenente sia il messaggio originale per intero, sia gli allegati con esso trasmessi (e dunque l'atto notificato e la relazione di notifica). In caso di esito negativo, invece, al posto della ricevuta di avvenuta consegna, viene generato un avviso di mancata consegna, rilevante per l'analisi delle ragioni che hanno determinato il mancato perfezionamento della notifica. Le ricevute di accettazione e avvenuta consegna (o l'avviso di mancata consegna) sono i documenti informatici da cui risultano l'invio, il compimento e l'esito della notificazione. Cfr. G. Ruffini (a cura di), *Diritto processuale civile*, vol. I, *La giustizia civile*, cit., 238 ss. per la prova in giudizio del compimento e dell'esito della notifica telematica.

card o chiavetta USB); disporre di un apposito *software* per la creazione della busta telematica, secondo le specifiche tecniche definite nel provvedimento del Direttore generale SIA; a questo riguardo si precisa che questi *software* sono disponibili sul mercato, avendo da tempo il Ministero fornito alle *software house* tutte le specifiche. Il Ministero non fornisce *software* per questa funzione, sebbene vi sia una serie di *software* gratuiti indicati sul sito del Portale dei Servizi Telematici[50].

4. Funzionalità non implementate e criticità.

Nel corso del tempo già trascorso dall'uso del PCT, soprattutto guardando alle funzioni relative alle procedure concorsuali, sono emerse alcune criticità e funzionalità non implementate.

In particolare, in passato è accaduto che a seguito del passaggio dal sistema del fallimento a quello della crisi d'impresa, il *software* che gestiva le procedure telematiche non era stato aggiornato rispetto ai nuovi termini stabiliti dal c.c.i.. Ciò poneva, soprattutto in passato un problema di responsabilità.

In realtà, anche alla luce dell'analisi finora redatta, ci si rende conto di come l'unica fonte per l'aggiornamento degli operativi da parte delle *software house* sia il Portale dei Servizi Telematici del Ministero della Giustizia, l'unico strumento in grado di rilasciare aggiornamenti, *patchworks*, certificati di cifratura, certificati *proxy* PdA e PST, le codifiche degli errori dei controlli etc. Infatti, il portale è l'unico strumento che, alle dipendenze del Ministero della Giustizia, ha la possibilità di rilasciare codici e strumenti vari per la modifica dei *software* privati usati dalle parti private. Il discorso è maggiormente stringente per la Consolle del Magistrato e per gli strumenti del cancelliere, in quanto gli stessi sono creati direttamente dal Ministero.

Altro problema riscontrato dalla prassi è stato quello dell'ostensione del fascicolo telematico della procedura da parte dell'imprenditore sottoposto a liquidazione giudiziale o alle altre procedure concorsuali. In realtà, come già

[50] https://pst.giustizia.it/PST/en/paginadettaglio.page?contentId=ACC655. In ordine ai depositi telematici nella crisi d'impresa (cfr. art. 40 c.c.i.), a titolo esemplificativo, attraverso le citate *software house* oppure attraverso il Dominio Giustizia, si possono compiere le seguenti funzioni: si seleziona il registro, ovvero quello delle procedure concorsuali; in ossequio alla normativa vigente, il rito da scegliere è quello che reca l'indicazione PU (ovvero: procedimento unitario). Il rito in questione può essere abilitato per l'accesso alle procedure di: declaratoria della liquidazione giudiziale, ammissione al concordato preventivo, omologa degli accordi di ristrutturazione, dichiarazione dello stato di insolvenza sia nei procedimenti di liquidazione coatta amministrativa che in quelli di amministrazione straordinaria, ristrutturazione dei debiti del consumatore, ammissione al concordato minore, omologa del piano di ristrutturazione e ammissione alla liquidazione controllata.
Per quanto riguarda la tipologia di atto, è necessario che la scelta ricada su quelli che recano indicazione del procedimento unitario (CCIPU). A prescindere dal software utilizzato, il rito e la tipologia di atto utilizzati devono far riferimento al procedimento unitario. Poiché lo scopo del procedimento unitario è la trattazione congiunta di tutti gli eventuali strumenti di regolazione della crisi e dell'insolvenza e dei ricorsi per liquidazione giudiziale depositati, in sede di deposito si può porre la seguente scelta. Se non si è a conoscenza della pendenza di altri procedimenti collegati ad una determinata parte (generalmente il medesimo debitore), il ricorso o in generale lo strumento di regolazione della crisi potrà essere depositato come atto introduttivo puro, senza l'inserimento di dati relativi ad altre procedure (verrà dunque abilitata la scelta "destinazione", che negli schemi ministeriali contraddistingue appunto tale tipologia di atto introduttivo). Laddove invece si sia a conoscenza della pendenza di un precedente procedimento si abiliterà la scelta "procedimento" e in tal modo si potranno inserire i riferimenti (R.G. e anno) della procedura già pendente al fine di consentire la riunione delle procedure, così come previsto dall'art. 40 c.c.i..

evidenziato la visibilità del fascicolo è appannaggio di tutte le parti costituite. Determinate problematiche possono riscontrarsi nella gestione dei flussi di cui sopra, ma sembrano essere molto rare e facilmente risolvibili con interventi direttamente delle cancellerie.

Il fulcro di tutte le problematiche di carattere pratico è incentrato sulla gestione da parte del Ministero della giustizia, l'unico in grado di correggere determinati errori e risolvere, con degli appositi aggiornamenti e note informative, l'interruzione del flusso interno/esterno.

Un problema di carattere generale, invece, sembra essere rappresentato dai rischi insiti nella sinteticità e nella standardizzazione[51].

Infatti, più problematiche sono le previsioni contenute nello schema di d.m. ai sensi dell'art. 46 disp. att. c.p.c. Qui non solo si avverte la tendenza a imporre una logica di uniforme e standardizzata redazione degli atti, ma vengono aprioristicamente stabiliti limiti dimensionali eccessivamente stringenti, che possono finire per comprimere l'esercizio del diritto di difesa. Piuttosto sfuggente è, poi, il requisito (di cui all'art. 8 del d.m.), in base al quale gli atti giudiziari debbono essere corredati dalla compilazione di schemi informatici conformi alle specifiche tecniche. Tale requisito, per essere conforme al dettato dell'art. 46 disp. att. c.p.c., dovrebbe esaurirsi nella previsione di soli campi destinati a contenere dati ed informazioni relativi al procedimento (tra cui, l'ufficio giudiziario, le parti, i difensori, il valore della controversia); tuttavia, non può non segnalarsi che lo stesso potrebbe preludere alla creazione di vere e proprie "griglie" o campi prestabiliti, anche quanto alle dimensioni, nei quali inserire, entro un determinato limite massimo di caratteri, i diversi contenuti dell'atto. Se questa fosse la direzione da intraprendersi[52], si sarebbe dinanzi a regole più invasive e limitanti dell'esercizio del diritto di difesa, quale primo passo verso futuri, nuovi allarmanti modelli di processo nei quali la lettura degli atti e il loro apprezzamento siano affidati alle macchine[53].

Anche gli atti del giudice, come visto, si presentano tendenzialmente in formato digitale (come veri e propri atti nativi digitali) e anche per essi sono previsti requisiti tecnici, sempre da concepirsi in base al principio di strumentalità. Per espressa previsione dell'ultimo comma dell'art. 46 disp. att. c.p.c.[54], infatti, le disposizioni dettate da tale articolo si applicano anche agli atti e ai provvedimenti del giudice in forma di documento informatico; tuttavia, l'art. 7 dello schema di d.m., attuativo dell'art. 46 disp. att. c.p.c., stabilisce da una parte, che il giudice redige i provvedimenti in modo chiaro e sintetico, nel rispetto dei criteri redazionali stabiliti dagli artt. 2 e 6 dello stesso schema di d.m. in quanto compatibili; dall'altra parte, che le dimensioni degli atti e dei

[51] G. Ruffini (a cura di), *Diritto processuale civile*, vol. I, *La giustizia civile*, cit., 176 ss.

[52] Eventualmente anche in occasione dei previsti futuri aggiornamenti con cadenza biennale del decreto ministeriale.

[53] G. Ruffini (a cura di), *Diritto processuale civile*, vol. I, *La giustizia civile*, cit., 176 ss. Inoltre, l'ultimo comma dell'art. 46 disp. att. c.p.c. esclude che il mancato rispetto delle specifiche tecniche sulla forma e sugli schemi informatici degli atti e l'inosservanza dei criteri e limiti di redazione si traducano in una invalidità dell'atto, ma al contempo non li ritiene irrilevanti, ammettendo che possano essere valutati dal giudice ai fini della decisione sulle spese del processo. Questa previsione, comunque, non consente di escludere, in base ai principi generali, che se la violazione di una specifica tecnica attiene effettivamente a un requisito indispensabile (si pensi, ancora una volta, alla sottoscrizione digitale o alla firma elettronica qualificata o all'assenza di elementi attivi, nel significato sopra precisato), l'atto possa essere invalido.

[54] Come inserito dall'art. 4, co. 3, lett. b, d.lg. n. 149/2022.

provvedimenti del giudice sono correlate alla complessità della controversia, anche in ragione della tipologia, del valore, del numero delle parti e degli interessi coinvolti.

Inoltre, il primo e il secondo comma dell'art. 196 *quinquies* disp. att. c.p.c.[55] stabiliscono che l'atto del processo redatto dal magistrato in formato elettronico è depositato in via telematica e che, se è formato da un organo collegiale, è sottoscritto con firma digitale anche dal presidente.

Tendenzialmente anche gli atti degli ufficiali giudiziari sono in forma di documento informatico, come gli atti dei cancellieri, dei segretari degli uffici giudiziari. Il requisito della sottoscrizione, espressamente previsto per gli atti compiuti dai cancellieri e dai segretari degli uffici (art. 196 *quinquies*, co. 3, disp. att. c.p.c.) non può che riguardare anche i primi (art. 196 *quinquies*, co. 1, disp. att. c.p.c.).

Per quanto riguarda il verbale di udienza in formato digitale, deve osservarsi che le funzionalità tecniche del processo telematico permettono che esso sia direttamente redatto dal magistrato tramite la *consolle*[56].

Una delle funzioni non ancora implementate e che riveste, nel quadro generale, una importanza fondamentale è l'assenza del dialogo completo con i vari registri, ovvero con le banche dati dell'Agenzia delle entrate, dell'INPS, del Registro delle imprese, nonché le informazioni risultanti dalla centrale rischi presso la Banca d'Italia, così come prescritto dal c.c.i.. Come già ricordato, al momento, c'è solo l'accesso diretto da parte dell'ufficiale giudiziario alle seguenti banche dati dell'Agenzia delle Entrate, attraverso il Sistema di Interscambio flussi Dati (SID): a) Dichiarazioni dei Redditi e Certificazione unica; b) atti del Registro; c) archivio dei Rapporti finanziari[57].

Infine, il punto forse nevralgico dell'implementazione del dialogo automatizzato tra i "flussi" interni ed esterni rimane sempre il fattore umano, come si avrà modo di sottolineare nelle conclusioni: infatti, emerge come una delle problematiche di maggior rilievo sia legata alla corretta ricerca del fascicolo nel registro e alla cultura informatica dell'avvocato e degli altri protagonisti del processo.

5. Analisi comparata nei principali paesi UE.

Per completare il quadro relativo allo stato di automazione, anche in virtù di una plausibile e futuribile creazione di un sistema unico e permeabile a livello euro unitario, si passeranno in rassegna i meccanismi di informatizzazione dei procedimenti civili nei principali paesi dell'Unione Europea.

[55] Articolo inserito dall'art. 4, co. 12, d.lg. n. 149/2022 e applicabile dal 1° gennaio 2023.

[56] Ovvero la scrivania multimediale che consente al giudice di interagire con tutti i dati costituenti il sistema informatico civile e di giovarsi di determinati strumenti pratici, come la possibilità di accedere, per i singoli procedimenti, a modelli di verbale già contenenti le indicazioni dell'ufficio giudiziario, delle generalità delle parti e del giudice, della data di udienza e del numero assegnato al procedimento. Laddove il verbale di udienza sia formato tramite *consolle*, non risulta tuttavia prevista la possibilità per soggetti diversi dal giudice di apporre la loro sottoscrizione digitale (il che vale anche per il cancelliere, la cui sottoscrizione, peraltro, come si è visto, non è considerata indispensabile dalla giurisprudenza).

[57] https://pst.giustizia.it/PST/en/dettaglio_schede_tematiche.page?contentId=ACC2849&modelId=12.

5.1. Germania.

In Germania, per i procedimenti civili, è possibile depositare una domanda o un'istanza per via elettronica all'organo giurisdizionale sotto forma di un documento elettronico. Tale domanda o istanza deve recare una firma qualificata della persona responsabile o (semplicemente) essere firmata dalla persona responsabile e presentata tramite un mezzo di trasmissione sicuro. I mezzi di trasmissione sicuri sono definiti all'articolo 130a, quarto §, dello ZPO[58].

Il documento elettronico deve essere adatto al trattamento. I parametri tecnici per la trasmissione e l'idoneità per il trattamento sono stabiliti nell'*Elektronische-Rechtsverkehr-Verordnung*[59].

I documenti giudiziari, in particolare le decisioni, possono essere notificati per via elettronica utilizzando mezzi di trasmissione sicuri (art. 173, 1 §, ZPO). Gli avvocati, i notai, gli ufficiali giudiziari, le autorità, le società e le istituzioni di diritto pubblico sono tenuti a mettere a disposizione un mezzo di trasmissione sicuro per la notificazione. Un documento elettronico può essere notificato a

[58] „§ 130a Elektronisches Dokument; Verordnungsermächtigung
(1) Vorbereitende Schriftsätze und deren Anlagen, schriftlich einzureichende Anträge und Erklärungen der Parteien sowie schriftlich einzureichende Auskünfte, Aussagen, Gutachten, Übersetzungen und Erklärungen Dritter können nach Maßgabe der folgenden Absätze als elektronische Dokumente bei Gericht eingereicht werden.
(2) Das elektronische Dokument muss für die Bearbeitung durch das Gericht geeignet sein. Die Bundesregierung bestimmt durch Rechtsverordnung mit Zustimmung des Bundesrates technische Rahmenbedingungen für die Übermittlung und die Eignung zur Bearbeitung durch das Gericht.
(3) Das elektronische Dokument muss mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden. Satz 1 gilt nicht für Anlagen, die vorbereitenden Schriftsätzen beigefügt sind.
(4) Sichere Übermittlungswege sind
1. der Postfach- und Versanddienst eines De-Mail-Kontos, wenn der Absender bei Versand der Nachricht sicher im Sinne des § 4 Absatz 1 Satz 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5 Absatz 5 des De-Mail-Gesetzes bestätigen lässt,
2. der Übermittlungsweg zwischen den besonderen elektronischen Anwaltspostfächern nach den §§ 31a und 31b der Bundesrechtsanwaltsordnung oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts,
3. der Übermittlungsweg zwischen einem nach Durchführung eines Identifizierungsverfahrens eingerichteten Postfach einer Behörde oder einer juristischen Person des öffentlichen Rechts und der elektronischen Poststelle des Gerichts,
4. der Übermittlungsweg zwischen einem nach Durchführung eines Identifizierungsverfahrens eingerichteten elektronischen Postfach einer natürlichen oder juristischen Person oder einer sonstigen Vereinigung und der elektronischen Poststelle des Gerichts,
5. der Übermittlungsweg zwischen einem nach Durchführung eines Identifizierungsverfahrens genutzten Postfach- und Versanddienst eines Nutzerkontos im Sinne des § 2 Absatz 5 des Onlinezugangsgesetzes und der elektronischen Poststelle des Gerichts,
6. sonstige bundeseinheitliche Übermittlungswege, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, bei denen die Authentizität und Integrität der Daten sowie die Barrierefreiheit gewährleistet sind.
Das Nähere zu den Übermittlungswegen gemäß Satz 1 Nummer 3-*bis* 5 regelt die Rechtsverordnung nach Absatz 2 Satz 2.
(5) Ein elektronisches Dokument ist eingegangen, sobald es auf der für den Empfang bestimmten Einrichtung des Gerichts gespeichert ist. Dem Absender ist eine automatisierte Bestätigung über den Zeitpunkt des Eingangs zu erteilen.
(6) Ist ein elektronisches Dokument für das Gericht zur Bearbeitung nicht geeignet, ist dies dem Absender unter Hinweis auf die Unwirksamkeit des Eingangs unverzüglich mitzuteilen. Das Dokument gilt als zum Zeitpunkt der früheren Einreichung eingegangen, sofern der Absender es unverzüglich in einer für das Gericht zur Bearbeitung geeigneten Form nachreicht und glaubhaft macht, dass es mit dem zuerst eingereichten Dokument inhaltlich übereinstimmt".

[59] V. il testo su https://www.gesetze-im-internet.de/ervv/.

chiunque altro soltanto se, in qualità di persona fisica, tale soggetto ha acconsentito alla notifica di documenti elettronici per i procedimenti in questione oppure se, in qualità di persona giuridica, tale soggetto ha fornito il proprio consenso generale alla notifica di documenti elettronici (art. 173, 4 §, ZPO)[60].

In generale, ciò che emerge dall'analisi della normativa tedesca è un sistema non sovrapponibile al PCT italiano, stante la preferenza per un sistema ancora "analogico" in vari Länder[61]. Ciò che colpisce, d'altra parte, è la digitalizzazione di alcuni servizi, soprattutto a livello amministrativo e, quindi, anche di amministrazione della giustizia, dove vi è un numero sempre più considerevole di banche dati e registri digitalizzati e, soprattutto, in comunicazione tra di loro, anche ad opera della *Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen* del 2017.

Infatti, il corrispettivo del Portale dei Servizi Telematici del Ministero della Giustizia in Germania è il portale della Giustizia Tedesca[62], dove sono contenuti una serie di servizi on-line, già operativi da diverso tempo in quasi tutti gli Stati Federati. Se, da una parte, la prima legislazione tedesca per l'introduzione dell'informatica nelle Aule giudiziarie degli Stati Federati è del 2001[63] e la firma elettronica qualificata e posta elettronica certificata sono utilizzate da più di tre lustri per lo scambio di atti e documenti nei processi e la procedura del decreto di ingiunzione telematico (secondo la legge tedesca che risulta differente da quella italiana, essendo prevista una prima fase completamente automatizzata) è operativa tramite formulario da compilare anche on line fin dal 2003[64], dall'altra parte spiccano forme di innovazione e interoperabilità come il catasto on line e la banca dati del Registro Imprese digitalizzata del

[60] „§ 173 Zustellung von elektronischen Dokumenten
(1) Ein elektronisches Dokument kann elektronisch nur auf einem sicheren Übermittlungsweg zugestellt werden.
(2) Einen sicheren Übermittlungsweg für die elektronische Zustellung eines elektronischen Dokuments haben zu eröffnen:
1. Rechtsanwälte, Notare, Gerichtsvollzieher, Steuerberater sowie
2. Behörden, Körperschaften oder Anstalten des öffentlichen Rechts.
Sonstige in professioneller Eigenschaft am Prozess beteiligte Personen, Vereinigungen und Organisationen, bei denen von einer erhöhten Zuverlässigkeit ausgegangen werden kann, sollen einen sicheren Übermittlungsweg für die elektronische Zustellung eröffnen.
(3) Die elektronische Zustellung an die in Absatz 2 Genannten wird durch ein elektronisches Empfangsbekenntnis nachgewiesen, das an das Gericht zu übermitteln ist. Für die Übermittlung ist der vom Gericht mit der Zustellung zur Verfügung gestellte strukturierte Datensatz zu verwenden. Stellt das Gericht keinen strukturierten Datensatz zur Verfügung, so ist dem Gericht das elektronische Empfangsbekenntnis als elektronisches Dokument (§ 130a) zu übermitteln.
(4) An andere als die in Absatz 2 Genannten kann ein elektronisches Dokument elektronisch nur zugestellt werden, wenn sie der Zustellung elektronischer Dokumente für das jeweilige Verfahren zugestimmt haben. Die Zustimmung gilt mit der Einreichung eines elektronischen Dokuments im jeweiligen Verfahren auf einem sicheren Übermittlungsweg als erteilt. Andere als natürliche Personen können die Zustimmung auch allgemein erteilen. Ein elektronisches Dokument gilt am dritten Tag nach dem auf der automatisierten Eingangsbestätigung ausgewiesenen Tag des Eingangs in dem vom Empfänger eröffneten elektronischen Postfach als zugestellt. Satz 4 gilt nicht, wenn der Empfänger nachweist, dass das Dokument nicht oder zu einem späteren Zeitpunkt zugegangen ist".

[61] Sul punto, cfr. Ampiamente B. HEIL, *IT-Anwendung im Zivilprozess. Untersuchung zur Anwendung künstlicher Intelligenz im Recht und zum strukturierten elektronischen Verfahren*, Tübingen, 2020, 9 ss.

[62] https://www.justiz.de/index.php;jsessionid=73CC732FE25F627572C00D0ECAE71896.

[63] Attraverso l'introduzione dell'art. 128a ZPO ad opera della *Gesetz zur Reform des Zivilprozesses vom* 27.7.2001.

[64] B. HEIL, *IT-Anwendung im Zivilprozess*, cit., 21 ss.

2022 (e v. *Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG)* e *Gesetz zur Ergänzung der Regelungen zur Umsetzung der Digitalisierungsrichtlinie (DiREG)*)[65]. Alla luce della stratificazione tedesca, composta da 16 stati, 130 Registri imprese e oltre 4.6 milioni di imprese, riunire tutto in un solo portale e per di più utilizzando standard operativi con accessi anche ai dati storici ha rappresentato un'impresa titanica, data anche la considerevole diversificazione dello stato dell'informatizzazione nei vari Länder[66].

Non esiste, però, né è in programma che venga in essere in tempi prossimi, un processo telematico come quello utilizzato in Italia nel settore civile, con l'obbligo di gestire il procedimento e le udienze in via telematica. Questo probabilmente si spiega con il fatto che l'informatica, se può aiutare la giustizia dal punto di vista strettamente amministrativo (i tempi di rilascio delle copie, la movimentazione dei fascicoli, la ricezione dei documenti ecc.), non ha una grande utilità con riferimento all'esercizio delle funzioni giurisdizionali in senso stretto. La redazione dei verbali avviene già in maniera efficiente ad opera dei cancellieri del giudice. Quest'ultimo registra, infatti, su appositi supporti magnetici l'udienza, il cui contenuto è, in seguito, trascritto con puntualità dai funzionari[67]

5.2. Francia.

La Francia non ha adottato il processo telematico per la formazione di fascicoli e replicazione dei processi su piattaforma online, ad eccezione che per il processo innanzi alla *Cour de Cassation*. Infatti, in Francia l'amministrazione della giustizia è organizzata su una struttura di tre livelli: 181 corti di prima istanza con giurisdizione generale, 473 corti di prima istanza con giurisdizione per i casi di minore importanza, 35 corti d'appello che decidono in fatto ed in diritto. I gradi di giustizia inferiore sono caratterizzati dall'oralità e non esiste quindi una piattaforma di processi ma esiste il cosiddetto *E-barreau* che è un sistema di comunicazione elettronica tra le corti e gli avvocati.

In particolare, il servizio *e-barreau* è l'interfaccia software che consente agli avvocati di comunicare in modo sicuro (grazie a un certificato) con le giurisdizioni. Possono controllare online lo stato dei loro procedimenti (solo con le Corti giudiziarie e d'appello) grazie alla rete privata virtuale per avvocati[68].

Assolutamente fuori dall'informatizzazione è stato lasciato il lavoro del giudice, sebbene siano state annunciate diverse riforme negli ultimi tempi, per digitalizzare il processo civile[69]. In ogni caso questa impostazione è stata ritenuta insufficiente in quanto tutto è lasciato alla volontarietà degli operatori del diritto di parteciparvi o meno, aderendo alla convenzione stipulata tra l'ordine degli avvocati ed il ministero di giustizia. Chi deciderà di aderire avrà in

[65] https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2022_Digitalisierungsrichtlinie.html.
[66] Il tutto è consultabile sul sito: www.handelsregister.de.
[67] Sul punto, v. G. CAVALLARI, *Brevi osservazioni sull'efficienza del sistema giudiziario penale e civile in Germania ed Italia: un confronto*, in *unicost.eu*, 22 maggio 2019.
[68] Cfr. M. VELICOGNA, A. ERRERA, S. DERLANGE, *e-Justice in France: the e-Barreau experience*, in *Utrecht Law Review*, 2011, 163 ss.
[69] https://www.ildubbio.news/giustizia/accordi-extragiudiziali-e-digitale-la-riforma-sul-civile-parla-anche-francese-ylxiali1.

dotazione una penna USB e delle credenziali per poter formare e firmare i documenti online.

In disparte, vi sono alcune spinte verso la digitalizzazione: si pensi alle *injonction de payer*, dove è prevista la totale dematerializzazione della fase monitoria del procedimento[70]; si pensi al rapporto in seno alla *loi n. 2019-222 de programmation 2018-2022 et de réforme pour la justice*[71], dove si parla di trasformazione digitale della giustizia, con tutte le conseguenze pratico-organizzative[72].

5.3. Spagna.

La Spagna rappresenta in questo quadro lo stato con un sistema digitale delle comunicazioni giudiziarie più risalente nel tempo. Infatti, con il Real Decreto 1065/2015, del 27 novembre 2015 "*sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET*", nel quadro della *Ley de Enjuiciamiento Civil* 42/2015, in riforma della *Ley 1/2000*, del 7 Gennaio[73].

Secondo l'art. 13 del Real Decreto 1065/2015, LexNET è un mezzo sicuro di trasmissione delle informazioni che, attraverso l'uso di tecniche crittografiche, garantisce l'invio di documenti e la ricezione di atti di comunicazione, la loro data di emissione, la disponibilità e la ricezione o l'accesso al loro contenuto. Allo stesso modo, il sistema LexNET garantisce il contenuto integrale delle comunicazioni e l'identificazione del mittente e del destinatario delle stesse mediante opportune tecniche di autenticazione, in conformità a quanto previsto dalla Legge 59/2003, del 19 dicembre, in materia di firme elettroniche, e dal Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Inoltre, il sistema LexNET è considerato un sistema di recapito elettronico certificato ai sensi dell'articolo 43 del Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014[74].

---

[70] https://www.service-public.fr/particuliers/vosdroits/F1746.

[71] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038261631.

[72] Sul tema C. BLÉRY e J-P. TEBOUL, *De la communication par voie électronique au code de cyber procédure civile*, in JCP, 2017, 665; C. BLERY e J-P. TEBOUL, *Une nouvelle ère pour la communication par voie électronique, in 40 ans après… Une nouvelle ère pour la procédure civile?*, in *Dalloz, coll. Thèmes et commentaires*, 2016, 31 s., n° 25; C. BLERY, *Securigreffe: l'identité numérique judiciaire opposable est née*, in *JCP*, 2016, 256; T. COUSTET, *Chantiers de la justice: 530 millions d'euros pour le virage numérique*, in *Dalloz actualité*, 1 aprile 2020, disponibile all'indirizzo https://www.dallozactualite.fr/flash/chantiers-de-justice-530-millions-d-euros-pour-virage-numerique#.XoQ7jIgzZPY. Si v. anche il rapporto dell'Institut Montaigne, Justice: *faites entrer le numérique*, novembre 2017, disponibile all'indirizzo https://www.institutmontaigne.org/ressources/pdfs/publications/justice-faites-entrer-le-numerique-rapport.pdf.

[73] Ovvero un pacchetto di riforma, al fine di snellire il processo civile, che è intervento sull'organizzazione dell'*Oficina Judicial* con lo scopo di "digitalizzare" la giustizia e di migliorare l'interoperabilità dei sistemi elettronici di gestione dei fascicoli nelle regioni.

[74] "Artículo 13. Definición y características.

1. El sistema LexNET es un medio de transmisión seguro de información que mediante el uso de técnicas criptográficas garantiza la presentación de escritos y documentos y la recepción de actos de comunicación, sus fechas de emisión, puesta a disposición y recepción o acceso al contenido de los mismos.

Le funzioni di LexNET sono il deposito e il trasporto delle memorie processuali e dei documenti di accompagnamento, nonché la loro distribuzione e trasmissione all'organo o all'ufficio giudiziario o pubblico competente per il loro trattamento; la gestione del trasferimento di copie, in modo che sulle copie siano accreditate la data e l'ora in cui è stato effettivamente effettuato il trasferimento agli altri avvocati comparenti e l'identità di questi ultimi, in conformità alle disposizioni delle leggi processuali; l'esecuzione di atti di comunicazione processuale in conformità con i requisiti stabiliti dalle leggi processuali; il rilascio di ricevute elettroniche, integrabili negli applicativi di gestione processuale, che attestino il corretto deposito delle memorie e dei documenti allegati, il trasferimento delle copie e l'invio e la ricezione degli atti di comunicazione processuale e, in ogni caso, la data e l'ora dell'effettivo svolgimento.

In definitiva, LexNet è un portale centralizzato gestito dal Ministero della Giustizia spagnolo a cui tutti gli avvocati abilitati sono automaticamente registrati[75]. A tale portale si accede con autenticazione (simili a quelli italiani); attraverso tale portale è obbligatorio veicolare tutti gli atti riguardanti il processo civile. L'obbligo, in vigore dal 1° gennaio 2016 è per tutte le cause dal valore superiore a 2000 euro dove è obbligatoria la presenza di un avvocato. La particolarità è che in Spagna è tutto gestito in modo centralizzato dal Ministero (a differenza dell'Italia dove, come visto, vi sono anche operatori privati).

6. Prospettive future.

La ricerca condotta sinora ha mostrato una serie di spunti, alcuni dei quali rappresentano dei nodi da sciogliere sia in chiave nazionale che in prospettiva euro-unitaria.

Premessa della riflessione è comprendere come con il PCT non si è in presenza di una nuova forma di processo civile[76]: «la forma telematica non è propriamente "forma" dell'atto […] bensì "ultra-forma", *corpus recipiens* dematerializzato di documentazione dell'attività processuale svolta, che non incide sullo scopo del processo e dei suoi atti, ma che impone *tout court* di fare ricorso a strumenti tecnologici di decrittazione dei *bit* di cui si compone la riproduzione informatica»[77]. Ciò consente di ridimensionare le problematiche di carattere squisitamente tecnico che, come si è avuto modo di approfondire, legano necessariamente la loro soluzione all'intervento ministeriale. Infatti, lo

Asimismo, el sistema LexNET garantiza el contenido íntegro de las comunicaciones y la identificación del remitente y destinatario de las mismas mediante técnicas de autenticación adecuadas, de conformidad con lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y en el Reglamento UE Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

2. El sistema LexNET tendrá la consideración de sistema de entrega electrónica certificada conforme al artículo 43 del Reglamento UE nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

3. Cuando el envío proceda de una Administración u organismo público y de las Fuerzas y Cuerpos de Seguridad podrá utilizarse el sistema de acceso mediante usuario y contraseña, siempre que la comunicación se realice a través de los Sistemas de Aplicaciones y Redes para las Administraciones".

[75] https://www.administraciondejusticia.gob.es/lexnet.

[76] C. PUNZI, *Sul processo civile telematico*, cit., 1 ss.

[77] A. TEDOLDI, *Il processo civile telematico tra* logos *e* techne, cit., 860.

sviluppo della giustizia elettronica comporta uno sforzo maggiore rispetto a quello identificabile da un punto di vista meramente operativo, come lo sviluppo, l'installazione e il collegamento di dispositivi tecnologici o la fornitura di un riconoscimento normativo all'uso del mezzo digitale al posto di quello tradizionale per lo scambio di documenti. La vera sfida non risiede nella ricerca, nell'assemblaggio e nella produzione di strumenti tecnologici, ma nella creazione della rete di *governance* di attori organizzativi rilevanti, necessaria per sostenere e implementare con successo l'innovazione. Si tratta di cercare compromessi accettabili su cosa si può fare e come si può fare.

La sfida, in misura maggiore, consiste nel trovare il modo di motivare gli utenti a partecipare attivamente alla creazione del nuovo servizio che non può funzionare senza di loro: il fattore umano gioca ancora un ruolo preponderante nella commissione di errori. Basti pensare alla gestione dei flussi, dove è l'avvocato a dover "ricercare" il provvedimento ed, eventualmente, a segnalare il malfunzionamento.

Infine, la vera criticità, soprattutto in materia di procedure concorsuali, si concentra nella incompiuta (anche se ancora *in itinere*) comunicabilità tra banche dati e sulla loro preventiva digitalizzazione.

Come noto, lo scambio di informazioni tra le autorità e l'accesso a informazioni in più lingue nell'UE è stato facilitato attraverso il sistema di interconnessione dei registri delle imprese (*BRIS*), che dà accesso ad oltre 20 milioni di società a responsabilità limitata dell'UE, e il sistema di interconnessione dei registri fallimentari (*IR1*)[78]. La direttiva (UE) 2019/1151[79] e la direttiva (UE) 2019/2121 [80] hanno introdotto nuovi requisiti per la digitalizzazione dei registri delle imprese e la fornitura di informazioni tra i registri delle imprese e al pubblico attraverso il BRIS[81].

Proprio la digitalizzazione e la "inter-comunicabilità" dei registri rilevanti ai fini della prevenzione della crisi (prima) e della liquidazione giudiziale (dopo) (e si pensi al registro delle imprese, ai dati dell'Agenzia delle Entrate, ai dati dell'INPS, ai dati bancari etc.) consentono di schiudere la prospettiva di una più stretta integrazione fra i mercati delle attività professionali e dell'opportunità di favorire il dialogo tra le piattaforme nazionali (sull'esempio dell'esperienza avviata in materia di pubblicità commerciale, prima attraverso forme di interconnessione fra i registri delle imprese ed ora con il progetto POS, in

[78] Regolamento (UE) 2015/848 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativo alle procedure di insolvenza (GU L 141 del 5.6.2015, p. 19).
[79] Direttiva (UE) 2019/1151 del Parlamento europeo e del Consiglio, del 20 giugno 2019, recante modifica della direttiva (UE) 2017/1132 per quanto concerne l'uso di strumenti e processi digitali nel diritto societario (GU L 186 dell'11.7.2019, 80).
[80] Direttiva (UE) 2019/2121 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva (UE) 2017/1132 per quanto riguarda le trasformazioni, le fusioni e le scissioni transfrontaliere (GU L. 321 del 12.12.2019, p. 1.
[81] Come noto, la direttiva consente di costituire una società e di registrare una succursale completamente online nonché di depositare, integralmente online, i documenti aziendali richiesti dai registri delle imprese. Questa direttiva fornisce funzionalità nuove al sistema di interconnessione dei registri delle imprese (*BR15*), compresi scambi nuovi di informazioni tra i registri delle imprese dell'UE: i) sugli amministratori interdetti; ii) su filiali transfrontaliere e su modifiche alle informazioni societarie; iii) su nuove serie di dati societari disponibili gratuitamente tramite l'interfaccia di ricerca sul portale europeo della giustizia elettronica. La direttiva (UE) 2019/2121 potenzia ulteriormente il BRIS con uno scambio nuovo di informazioni tra i registri delle imprese dell'UE e informazioni pubbliche nuove in merito a conversioni, fusioni e scissioni transfrontaliere.

considerazione fra l'altro della proposta di Direttiva del 7 dicembre 2022 sulla disciplina euro-unitaria dell'insolvenza) [82] . In tal guisa, risultano utili le pionieristiche indicazioni fornite dalla proposta di Direttiva relativamente al reimpiego di strumenti telematici istituiti dall'Unione quali l'accesso alle banche dati e i "prospetti in-formativi" per il portale *e-Justice*. In particolare, sono da considerare rilevanti le disposizioni contenute nei Titoli III e VIII, dove le prime sono volte a consentire agli "*insolvency practitioner*" la consultazione delle banche dati decentrate costruite dagli Stati membri sulla scorta delle direttive "antiriciclaggio" [83] , al fine di "identificare e tracciare i beni appartenenti all'attivo della procedura, inclusi quelli assoggettabili ad azione revocatoria" (artt. 14,§ 1 e 15, §§ 1 e 17), oltre che di tutti i *database* composti su iniziativa dei singoli Stati membri, contenenti dati utili per ricostruire la composizione del patrimonio del debitore assoggettato a procedura[84]. Inoltre, in disparte le norme di protezione dei dati e quelle tipiche dell'antiriciclaggio, tutti i *practitioner*, indipendentemente dallo Stato membro in cui si svolga la procedura cui sono preposti, avranno modo di consultare qualsiasi banca-dati ovunque istituita, tramite i sistemi centralizzati di interconnessione (là dove predisposti dalla Commissione), oppure la singola banca dati decentrata, con la clausola della non discriminatorietà (art. 18)[85].

Si prevede che la consultazione, però, non potrà sempre avvenire in maniera diretta, in quanto la visione dei dati contenuti nei registri centralizzati dei conti bancari sarà mediata dall'intervento del tribunale fallimentare, che dovrà caso per caso vagliare l'opportunità di trasmettere al *practitioner* i dati richiesti.

L'art. 68, nel titolo VIII, invece, assegna a ciascuno Stato il compito di mettere a disposizione degli investitori (per mezzo dell'"Atlante giudiziario europeo in materia civile" ospitato nel portale web "*e-Justice*"[86]) un prospetto informativo chiaro, sintetico, accurato e aggiornato, contenente informazioni essenziali relative al proprio regime concorsuale e redatto secondo una griglia standard. Idealmente, l'iniziativa punta a colmare quantomeno le più rilevanti asimmetrie informative che normalmente affliggono gli investitori intenti a ponderare il rischio d'insolvenza di un debitore straniero[87]. I prospetti commissionati agli Stati membri dovranno strutturarsi in quattro sezioni, concernenti gli aspetti cui, si assume, gli investitori guardano con maggiore attenzione, ovvero: 1) le

---

[82] Sul tema, v. M. LAMANDINI, *Prospettive europee in tema di assemblee virtuali e comunicazioni con i soci*, in N. ABRIANI e R. COSTI (a cura di), *Diritto societario, digitalizzazione e intelligenza artificiale*, Milano, 2023, 37 ss., spec. 39 ss.; ma v. anche L. BENVENUTO, F. SAVASTA, *La digitalizzazione delle informazioni finanziarie nel Regolamento ESEF e le prospettive di accesso unitario e comune alle stesse*, in M. BIANCHINI, G. GASPARRI, G. RESTA, G. TROVATORE, A. ZOPPINI (a cura di), *Gli sviluppi tecnologici del diritto societario*, quaderno Consob, maggio 2022, n. 23, 10 ss.

[83] Il Registro nazionale centralizzato dei conti bancari (costituente una sezione dell'Anagrafe tributaria, ed è istituito in osservanza dell'art. 32 *bis* della Direttiva (UE) 2015/849) e il Registro dei titolari effettivi (previsto dell'art. 21 d.lg. 21 novembre 2007, n. 231, che recepisce l'art. 31, par. 3 *bis* della citata direttiva).

[84] L'elenco di queste banche dati sarà contenuto in un futuro allegato alla direttiva.

[85] È stato affermato che «Quest'ultima previsione costituisce, evidentemente, uno sprone affinché gli Stati membri sopperiscano all'assenza di un sistema d'interconnessione europeo dematerializzando, quanto più possibile, le modalità di accesso alle proprie banche dati decentrate; quello telematico rappresenta, infatti, il metodo di consultazione meno discriminatorio, essendo egualmente accessibile a tutti gli utenti, indipendentemente dalla loro collocazione geografica», così K. SILVESTRI, *La proposta di direttiva del Parlamento europeo e del Consiglio sull'armonizzazione di taluni aspetti del diritto dell'insolvenza*, in *dirittodellacrisi.it*, 17 gennaio 2023.

[86] https://e-justice.europa.eu/home?action=home&plang=it.

[87] V. considerando 58 della proposta di Direttiva in commento.

condizioni di apertura delle procedure d'insolvenza[88]; 2) i procedimenti di insinuazione, verificazione e ammissione dei crediti[89]; 3) la distribuzione del ricavato[90]; 4) la durata media delle procedure[91].

In fin dei conti, ciò che rileva è ancora una volta il fattore umano e l'umana "ricerca" dei dati, a patto di non voler lasciare tutto alle macchine; del resto Ivan, negli anni venti del secolo scorso, affermava: «finora noi russi abbiamo a che fare con materiale umano primitivo. Siamo costretti ad adattare l'aereo al tipo di pilota di cui disponiamo. In tanto in quanto riusciremo a addestrare un altro tipo umano, potremo perfezionare anche lo sviluppo tecnico del materiale. I due fattori si condizionano reciprocamente. Non si possono piazzare uomini primitivi in macchine complicate»[92].

[88] Tale sezione dovrà riferire chi siano i soggetti legittimati a richiedere l'apertura delle procedure d'insolvenza; quali siano i requisiti soggettivi e oggettivi per l'apertura; i criteri per determinare il giudice o l'autorità competente; le modalità di convocazione del debitore.

[89] Tale sezione dovrà specificare quali diritti possano venir insinuati al passivo della procedura e a quali condizioni; descrivere le tempistiche e le modalità della presentazione della domanda di ammissione; indicare il giudice o l'organo della procedura competente a ricevere le domande; sunteggiare le cadenze del procedimento di verifica.

[90] Questa sezione dovrà offrire agli investitori una sinossi dell'ordine di distribuzione del ricavato, all'interno della quale poter individuare la propria posizione, nonché una succinta descrizione del procedimento di distribuzione.

[91] La durata media delle procedure dovrà essere misurata sulla scorta dei dati che gli Stati membri debbono raccogliere e aggregare, su base annua e nazionale, in osservanza dell'art. 29, par. 1, della Direttiva "*Insolvency*".

[92] H. SPEIDEL, *Reichswehr und Rote Armee*, in *Vierteljahrshefte für Zeitgeschichte*, Institut für Zeitgeschichte, I, n. 1, 1953, 38. V. vfz.ifz-muenchen.de.

Owusu A, 'Data sharing in the personal data economy. Does sharing mean caring?' (2023) 2 EJPLT, 217 - 239.
DOI: https://doi.org/10.57230/EJPLT223AO

EJPLT
ISSN 2704-8012



Data sharing in the personal data economy. Does sharing mean caring?

La condivisione dei dati nell'economia dei dati personali. Condividere vuol dire prendersi cura?

ABIGAIL OWUSU
Postdoctoral Research Fellow
University of Verona
Lawyer

Abstract

Following its approval by the European Parliament in April 2022, the Data Governance Act (DGA) introduces regulation for the providers of data intermediation services. The Regulation seeks to empower data subjects and ensure the competitiveness of the markets in which data intermediaries operate. After providing the necessary background, this paper aims at offering a first general overview, from a private law standpoint, on both merits and limitations of the regulatory approach on data sharing adopted by the DGA. It outlines questions that need to be addressed in order to verify that the Regulation delivers the benefits it promises.

In seguito alla sua approvazione, nell'aprile 2022, da parte del Parlamento europeo, il Data Governance Act (DGA) ha introdotto una normativa rivolta ai fornitori di servizi di intermediazione dei dati. Il regolamento mira a garantire agli interessati maggior controllo sui propri dati, nonché la competitività dei mercati in cui operano gli intermediari di dati. Il presente saggio, svolte alcune doverose premesse, intende offrire una prima panoramica generale sui pregi e sui limiti dell'approccio normativo, adottato dal DGA, al tema della condivisione dei dati, dal punto di vista del diritto privato. Lo scritto individua le questioni che devono essere affrontate al fine di verificare se il regolamento è realmente idoneo a perseguire i benefici promessi.

© The author(s) 2023, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Data protection; Personal data; Non-personal data; Data sharing; Data intermediation services; Data Intermediaries; Commodification of personal data; Fundamental human rights.

Summary: Introduction. – 1. The background of the Regulation and the European Data Strategy. – 2. Types of data intermediaries. – 3. The DGA framework: subject matter, scope of application and definitions. – 4. Conditions for providing data intermediation services. – 5. The enforcement mechanism. – 6. Risks of data sharing and the limits of the DGA. – Conclusions

Introduction.

Access to big data plays a crucial role for societal development. The availability of vast datasets enables data analysts to make accurate predictions in different business sectors, such as marketing and finance, tackling major challenges. Access to data is also extremely important in the context of Artificial Intelligence, since machine learning cannot take place without the availability of a large amount of data. Having access to data is a powerful tool to gain business advantage over competitors.

The question on how the governance of this data should be designed i.e. who has control over this data, who can use it, and who can benefit from its value is a key policy question for the development of the European data economy. It does not come as a surprise that data regulation in general and the debate on access to and ownership of data, in particular, have become the most visible regulatory discussions in recent EU regulatory policies.

This paper presents the result of a legal analysis of the European Commission's Data Governance Act (DGA), which entered into force on June 23, 2022, and is applicable since September 24, 2023, with respect to the provision of «data intermediation services».

According to the new Regulation, data intermediaries are expected to facilitate data sharing within the EU, by that means increasing the amount of data available to European businesses for their activities. On the other hand, due to the central role within the European data economy that data intermediaries, as two-sided platforms, will occupy, the EU legislator is aware of the risks for users and competition at large. In this perspective, the DGA is aimed both at establishing trust in data intermediaries, thereby strengthening their role, and, simultaneously, at pre-emptively limiting potential abuses.

The reactions of academics and stakeholders to the DGA are very ambivalent. Although many are welcoming the objectives and the basic approach of the DGA, there is an increasing awareness that the new Regulation also entails a lot of challenging problems. In addition to many unclear provisions and concerns about costs of compliance, open questions about the risks of the commodification of personal data, and the dangers of new forms of data concentration and data power have been raised.

Furthermore, crucial questions on its relationship with data protection law and the necessity of such a far-reaching horizontal regulation have emerged in

this discussion.

This paper intends to contribute to this debate by providing a preliminary analysis of the effects of the provisions in the DGA with respect to its objectives. This entails, in particular, an analysis of the ex-ante obligations imposed on data intermediation services, and whether they can be expected to be sufficiently effective for achieving its objectives. However, it also requires a broader critical analysis of the effects of the specific model of data governance envisaged in the DGA, which should enable all data holders and users to participate in the economic value created by intermediation services.

The paper is structured as follows: Section I will present some background on the governance problems of data, and on how the European Data Strategy was conceived. Section II describes different data sharing models and the corresponding market developments in the absence of specific regulation. Against this background, the subsequent sections of the paper focus on the architecture of the DGA, illustrating the subject matter, its scope of application, definitions, enforcement mechanisms, and, most importantly, the ex-ante obligations imposed on data intermediation services. Section VI discusses the risks of data sharing and the limits of the DGA. The last section draws some conclusions.

1. The background of the Regulation and the European Data Strategy.

In recent years, data-driven technologies have had transformative effects on all sectors of the economy.

The proliferation of products connected to the Internet of Things in particular has increased the volume and potential value of data for consumers, businesses, and society.

The ability to store, arrange, and analyze data in order to gain insights is what gives data its enormous financial value.[1]

Data markets consist of three main links along the data value chain: collection, synthesis and analysis, and use.[2]

The collection of data relates to the recording, aggregation, and organization of information into a form that can be used for data mining.[3]

Synthesis and analysis relate to the integration of different types of data and the analytical processing of data in order to find correlations.[4]

[1] OECD, Data-Driven innovation: Big data for growth and well-being (2015) 150, https://www.oecdilibrary.org/science-and-technology/data-driven innovation_9789264229358-en.

[2] N Elkin-Koren, MS Gal, The Chilling Effect of Governance-by-Data on Data Markets, (2019) 86(2) The University of Chicago Law Review, 410, https://chicagounbound.uchicago.edu/uclrev/vol86/iss2/6.

[3] See KJ Strandburg, 'Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context', in J Lane (ed.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge, 2014), 5, 10 ff.

[4] Elkin-Koren, Gal, 'The Chilling Effect of Governance-by-Data' 410.

The last link, use, involves utilizing data-based information to improve decision-making in order to innovate[5] or to increase productivity.[6] For example, personal data can be used to create a digital profile for each individual, which could then be used to improve personalized products and services or for microtargeted advertising.[7]

What sets data apart from other resources is their re-usability: the great value of data lies in their nature as non-rivalrous goods. Multiple businesses can use the same data simultaneously or subsequently for their individual purposes without its value diminishing.[8]

Data are also considered multi-purpose inputs, i.e. useable for a multitude of different purposes, many of which cannot be anticipated a priori.[9]

Because of the economic and societal value of data, the European Commission issued a communication called «A European strategy for data» in 2020, announcing the «aim to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint».[10]

Stimulating the use of data in various sectors of the economy is key to creating the EU data economy.[11] Currently, the use and sharing of data is negatively influenced by several factors such as the insufficient availability of data, imbalances in market power, insufficient governance structures and technical infrastructures, or the lack of adequate tools that would empower consumers to make use of their rights that rely upon the sharing of data (i.e., data portability rights).[12]

The initiatives that have fostered the development of the European data economy are the Regulation (EU) 2022/868 on European data governance (Data Governance Act),[13] the Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act),[14] and the Regulation

[5] T Niebel, F Rasel, S Viete, 'BIG data – BIG gains? Understanding the link between big data analytics and innovation' (2019) 28(3) Economics of Innovation and New Technology, 296 ff. https://doi.org/10.1080/10438599.2018.1493075.

[6] E Brynjolfsson, W Jin, K McElheran, 'The power of prediction: Predictive analytics, workplace complements, and business performance' (2021) 56(4) Business Economics, 217 ff., https://doi.org/10.1057/s11369-021-00224-5.

[7] See S Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology, 78-79.

[8] OECD, Data-Driven innovation: Big data for growth and well-being, 179; see also B Custers, D Bachlechner, 'Advancing the EU data economy: Conditions for realizing the full potential of data reuse' (2017) 3-4, https://ssrn.com/abstract=3091038.

[9] OECD, Data-Driven innovation: Big data for growth and well-being, 181.

[10] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A European strategy for data' [COM(2020)86 final].

[11] European Commission, A European strategy for data, 1-2.

[12] ibid 6 ff.

[13] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[14] Regulation (EU) 2022/1925 of The European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

(EU) 2022/1925 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).[15]

The Data Governance Act, which will be applicable as of September 24, 2023, is the first legislative instrument announced in the European Data Strategy to come into force. The DGA aims to facilitate the re-use and sharing of data in and between the private and public sectors.

The apex of the European Commission's regulatory initiatives for the data economy is the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) [COM/2022/68 final] published on February 23, 2022.[16] The Data Act (DA) is another building stone for a regulatory framework to support data access and its re-use in view of consolidating a European data space that guarantees a high level of data protection.

2. Types of data intermediaries.

At various stages of the data life cycle, it has become increasingly common for businesses to rely upon third-party services. More precisely, data intermediaries have emerged as a new type of third-party services addressing the sharing of data between consumers and businesses (C2B) as well as between businesses themselves (B2B).

The two most important types of B2B data intermediaries potentially covered by the DGA are data marketplaces and industrial data platforms.[17]

Data marketplaces correspond to the classic model of a two-sided matching platform: on data marketplaces, data holders can offer their data to potential data users, while users can search different data offerings to find the purpose-specific data they need.[18]

Data marketplaces are in principle open and therefore target a wide and unknown range of participants.[19]

---

[15] Regulation (EU) 2022/2065 of The European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[16] European Commission, Proposal for a Regulation of The European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) [COM/2022/68 final], Bruxelles, 23.2.2022. On November 9, 2023, the European Parliament has adopted the final version of the Data Act. The Act is now subject to formal approval by the Council and once adopted, will enter into force 20 days after Official Journal publication, becoming applicable after 20 months.
On the Data Act proposal, see Fernandez, 'The Data Act: the next step in moving forward to a European Data Space' (2022) 8(1) European Data Protection Law Review, 108-114; Gallese, 'A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act) (2022) 3 Media Laws, 237-270; Leistner, Antoine, 'Attention, here comes the EU Data Act! A critical in-depth analysis of the Commission's 2022 Proposal' (2022) 13(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 339-349; Kerber, 'Governance of IoT Data: why the EU Data Act will not fulfill its objectives' (2023) 72(2) GRUR International, 120-135.

[17] European Commission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Building a European data economy. Commission, Free flow of data. SWD/2017/2 final, 17.

[18] See P Koutroumpis and others, 'Markets for data' (2020) 29(3) Industrial and Corporate Change, 647, https://doi.org/10.1093/icc/dtaa002. Dawex (https://www.dawex.com/en/) is an example of a platform for matching supply and demand for individual data. Its services are essentially limited to finding the right buyer for a company that wants to monetize data it holds.

[19] L von Ditfurth, G Lienemann, 'The Data Governance Act: – Promoting or Restricting Data Intermediaries?' (2022) 23(4) Competition and Regulation in Network Industries, 274, https://doi.org/10.1177/17835917221141324; H Richter, PR Slowinski, 'The data sharing economy: On

In addition, data marketplaces may become much more than a mere enabler for data sharing, should it offer additional services like anonymization and adjust the data to specific business needs of the companies.[20]

The other important type of data intermediaries falling within the scope of the DGA are so-called industrial data platforms. [21] Unlike with data marketplaces, the main purpose of industrial data platforms is to provide the technical infrastructure for companies to share data with each other as part of their broader collaboration.[22] It is also common to speak of "data pooling": participants enter certain data into the data pool and in return receive access to the data fed into the pool by the other participants, thereby increasing the amount of data available for all of the participants.[23]

Furthermore, data spaces serve as the fast and secure infrastructure for individual data exchanges among their users.[24]

Industrial data platforms can be open or closed. In the case of open platforms, participation is open to all companies that meet certain criteria. Closed platforms, on the other hand, restrict participation to certain cooperating firms.[25]

Somewhere in between entirely "open" and "closed" platforms are those which allow sharing between specific companies, while the "data sharing club" is open to new entrants if they fulfill certain requirements.[26]

Other forms of B2B-data intermediaries are data cooperatives and data brokers.

Data cooperatives store and aggregate data for their users – typically small businesses from specific sectors – and enable them to manage their data in a self-determined and informed manner.[27]

Data brokers are the most established and commercially successful type of data intermediary as they collect and aggregate data from a wide range of sources (including businesses) and then sell the aggregated data to third parties.[28]

The most common type of C2B data intermediaries are Personal Information Management Services (PIMS).

---

the emergence of new intermediaries' (2019) 50(1) International Review of Intellectual Property and Competition Law, 12, https://doi.org/10.1007/s40319-018-00777-7.

[20] Richter, Slowinski, 'The data sharing economy' 12.

[21] European Commission, Document on the free flow of data, 18.

[22] European Commission, Study on data sharing between companies in Europe (2018) 62, https://op.europa.eu/de/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

[23] A Wernick, C Olk, and M Grafenstein, 'Defining data intermediaries. A Clearer View through the Lens of Intellectual Property Governance' (2020) 2 Technology and Regulation, 74, https://doi.org/10.26116/techreg.2020.007.

[24] European Commission, Study on data sharing, 62.

[25] L von Ditfurth, G Lienemann, 'The Data Governance Act' 275.

[26] H Richter, PR Slowinski, 'The data sharing economy' 12. An interesting example of this type of platform is iShare (https://hollandfintech.com) which enables everyone in the logistics sector to share information with all participants.

[27] M Jouanjean and others, 'Issues around data governance in the digital transformation of agriculture: The farmers' perspective', in *OECD Food, Agriculture and Fisheries Papers* 146 (OECD Publishing, 2020) 15 ff., https://doi.org/10.1787/53ecf2ab-en.

[28] OECD, Enhancing Access to and sharing of data: Reconciling risks and benefits for data Re-use across societies (2019) 37, https://www.oecd-ilibrary.org/science-and-technology/enhancing-access-to-andsharing-of-data_276aaca8-en.

PIMS are intermediaries in the sense that they endeavor to connect to different ends of the markets by obtaining a commitment from data-generating companies to provide a "data handback" (i.e., a copy of the personal data) to consumers, so that the data can be stored, managed and shared with third parties through the PIMS ecosystem.[29]

In addition to providing secure spaces for the collation of personal information, PIMS increasingly provide additional functionalities such as profiling, automatic form completion, certification/verification services, a central digital letterbox for sharing information with, and receiving data from, controls to help consumers manage and filter what information they share, and to create personal profiles that they can share and use to make more informed decisions across the web.[30]

An early example of PIMS is a program called "Lumeria": a customer will store personal data in a SuperProfile. The more specific the information stored (about such things as age, sex, family status, etc.), the more valuable that profile will become to advertisers, who will pay handsomely to participate in Lumeria's network. In exchange Lumeria will give them the chance to do highly targeted, permission-based marketing to offer special deals on services to people of a predetermined demographic profile. Most of the money will go directly to Lumeria's users and Lumeria will take a small cut.[31]

Similarly, the Weople app, which is operated by an Italian company called Hoda srl, encourages web users to link third-party accounts (such as Gmail and other Google accounts) to port their personal data into a "digital vault" — where their data will be «masked and anonymized» so that it can be used to target them with personalized offers.[32] Weople users are able to generate virtual currency or other rewards and potentially earn actual money, in exchange for authorizing the use of their "masked" data for marketing purposes. The app also aggregates anonymized user data into blocks to trade with marketers.

PIMS are advertised as empowering individuals to obtain value from their personal data by selling or providing access to their personal data to data buyers.

From a data protection perspective, PIMS can serve as a means to declare consent and invoke the rights of access, erasure, rectification and portability on behalf of data subject.[33]

---

[29] N Zingales, 'The Rise of 'Infomediaries' and Its Implications for Antitrust' (ASCOLA, 2017) 21.
[30] ibid 21-22.
[31] T Lester, 'The Reinvention of Privacy' 2001 Atlantic Monthly 287(3), 36.
[32] Cf. weople.space/en/#functions. There have been concerns over Weople's approach of leveraging GDPR data portability rights to grease the commercial tradability of personal data.
Back in 2019, the app was referred to the European Data Protection Board (EDPB) by the Italian data protection authority (Garante per la Protezione dei Dati Personali), for an opinion on its approach to utilizing the GDPR's data subject portability rights to make money (Garante per la protezione dei dati personali, Dati in cambio di soldi: il Garante privacy porta la questione in Europa. Sotto la lente dell'Autorità la app "Weople", 1 August 2019, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9126709). Later, the EDPB sent a letter to Weople, stating that the «request for an opinion […] was withdrawn by the Italian Supervisory Authority, and therefore the EDPB is no longer drafting such an opinion» (EDPB Secretariat, Response to Hoda letter, 21 January 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_responsetohodaletter_final_0.pdf).
[33] von Ditfurth, Lienemann, 'The Data Governance Act' 275-276.

3. The DGA framework: subject matter, scope of application and definitions.

As mentioned in the previous sections, data intermediation services play a key role in the data economy, in particular in supporting and promoting voluntary data sharing practices between businesses. In the view of the EU legislator, «data intermediation services providers, which may include public sector bodies, that offer services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediation services that are independent from data subjects, data holders and data users could have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power, while allowing non-discriminatory access to the data economy for undertakings of all sizes, in particular SMEs and start-ups with limited financial, legal or administrative means. This will be particularly important in the context of the establishment of common European data spaces, namely purpose or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives».[34]

On this premise, the DGA aim «to improve the conditions for data sharing in the internal market, by creating a harmonised framework for data exchanges and laying down certain basic requirements for data governance, paying specific attention to facilitating cooperation between Member States»,[35] with the ultimate goal of further developing «the borderless digital internal market and a human-centric, trustworthy and secure data society and economy».[36]

In addition to regulating data intermediaries (Arts. 10 – 15), the DGA also addresses the re-use of data held by the public sector (Arts. 3 – 9), and it further contains special rules for organizations that require and use personal data for altruistic purposes (Arts. 16 – 25).

This paper exclusively focuses on the regulation of data intermediation services: its goals, its enforcement mechanisms and, most importantly, its conditions for providing data intermediation services.

The main activity regulated by the DGA, i.e. data sharing, is defined as «the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge».[37]

Other than the data subject as referred to in Art. 4 (1) GDPR, two are the new subjects to whom the Regulation is addressed: the «data holder» and the «data user».

The data holder is the «legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable

[34] Cf. Recital 27 DGA.
[35] Cf. Recital 3 DGA.
[36] ibid.
[37] Art. 2 (10) DGA

Union or national law, has the right to grant access to or to share certain personal data or non-personal data».[38]

Data user means «a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non- commercial purposes».[39]

In their joint opinion on the DGA proposal, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) shared their concerns on the existing tension between data protection principles and data sharing.[40] In this joint opinion the two authorities highlighted a number of inconsistencies between the GDPR and the DGA proposal.

As far as the terminology is concerned, the joint opinion noted the confusion and incompatibility between the notion of «data holder» under the DGA proposal and that of «data subject» in the GDPR, and between the notion of «data user» under the DGA proposal and that of a «data controller» under the GDPR: in both these cases, there could be conflicts between the rights and prerogatives derived from these partially overlapping concepts.[41]

The joint opinion concluded that the DGA proposal «does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law»,[42] and therefore «raises serious concerns from a fundamental rights viewpoint».[43]

The above-mentioned concerns where endorsed by some academics.[44]

Although the transition between the November 2020 version of the DGA proposal and the subsequently dismissed version show a rethinking of the new language adopted, by maintaining alongside the «data holder» and the «data user» the notion of «data subject» as referred to in Art. 4 (1) GDPR), the EU regulatory evolution toward the commodification of personal data is undeniable. As it will be further discussed, the new trend is confirmed, among other things, by the reference to the possibility of data recovery in the event of insolvency of the data intermediation services provider (Art. 12 (h) DGA).

By affirming that the «data holder» has the right to grant access to or to share certain personal data or non-personal data in favor of «data users» the DGA also emphasizes another legal status, i.e. those of «data users», who have their own individual legal position, which can be qualified in various ways, depending on how the processing of data takes place, and are, therefore, difficult to define a priori.[45] The reference to the GDPR indicates cases where the «data user» already has, as the «data controller», autonomous legal

[38] Art. 2 (8) DGA.
[39] Art. 2 (9) DGA.
[40] EDPB and EDPS, EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act) (2021), 8 ff., https://edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/edpb-edps-joint-opinion-proposal_en.
[41] EDPB and EDPS, EDPB-EDPS Joint Opinion 03/2021, 9 ff.
[42] EDPB and EDPS, EDPB-EDPS Joint Opinion 03/2021, 7.
[43] ibid.
[44] See F Bravo, 'Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act' (2021) 1 Contratto e impresa Europa, 239 ff.
[45] ibid. 241.

situations over such data, by virtue of the legal bases set forth in Articles 6(1) and 9(2) GDPR.[46]

The user's rights to access and use data generated by IoT devices and to share such data with third parties are expressly regulated by the Data Act[47].

Art. 2 (11) DGA, defines the data intermediation service as «a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means (…)».

In order to be classified as a provider of data intermediation services, it is not sufficient to merely provide the technical tools for data sharing without the aim to establish or gather information on commercial relationships between data holders and users.[48]

The DGA identifies three types of data intermediation services.

The first category includes «intermediation services between data holders and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders with data users».

Data marketplaces are typically covered by the definition of Art. 2 (11) DGA.[49]

Open industrial data platforms may fall within the scope of application of Art. 2 (11) DGA, if they assist in the establishment of commercial relationships and do not merely assist with the technical aspects of data sharing.[50]

Data intermediaries that do not establish direct relations between data holders and data users – which prominently includes data brokers[51] – are excluded from the scope of application of the DGA.

It is surprising that the DGA does not apply to the most established and commercially successful type of data intermediary.

Furthermore, it is necessary for a data intermediary to aim at establishing relations between an undetermined number of data holders and users.

---

[46] F Bravo, '«Destinatario» dell'informazione e trattamento dei dati personali nell'evoluzione dell'ordinamento europeo', in M D'Auria (ed.), I problemi dell' informazione nel diritto civile, oggi studi in onore di Vincenzo Cuffaro (Roma TrE-Press, 2022), 454.

[47] Art. 4 (1) DA « Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible».
Art. 5 (1) DA « Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9».

[48] Cf. Recital 28 DGA.

[49] ibid.

[50] von Ditfurth, Lienemann, 'The Data Governance Act' 280.

[51] Ibid.

Therefore, the DGA does not cover closed services which are only available to a single data holder or to a pre-selected group of businesses.[52]

According to Art. 10 (a) DGA, providers of technical or other means for enabling data intermediation services are themselves considered data intermediaries under the DGA. Nevertheless, pursuant to Recital 28 DGA, such providers only fall within the scope of the regulation if the provision of such tools is either aimed at establishing a commercial relationship or allows them to acquire information on the establishment of commercial relationships.

Ordinary cloud services, data sharing software, web browsers or email services are not covered by the Regulation.[53]

Art. 10 (b) explicitly addresses C2B intermediaries which provide «intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users, including making available the technical or other means to enable such services, and in particular enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679».

This category includes PIMS and related services.

Such data intermediation services providers assist data subjects in exercising their rights under the GDPR, in particular giving and withdrawing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, the right of erasure or right "to be forgotten", the right to restrict processing and the right to data portability. In this regard, the DGA deems crucial that the business model of such providers ensures that there are no misaligned incentives that encourage data subjects to use such services to make more data relating to them available for processing than would be in their interest.[54]

The language of the provision is reminiscent of art. 80 GDPR which facilitates the defence of the rights of data subjects by accepting mandates for non-profit organisations.[55]

Data subjects, by law, can now give a power of attorney [56] to data intermediation services providers, which acts in force of a contract of mandate.

This provision is introduced for legal systems that do not have an existing discipline regarding mandate, and, in legal systems where this contract already exists,[57] to force by law data intermediation services providers to promptly comply with that mandate.

Thanks to this new provision, the possibility to use a mandate and the obligation to comply are clearly laid out by law.

Lastly, Art. 10 (c) DGA includes data intermediation services provided by data cooperatives (as defined in Art. 2 (15) DGA) into the scope of application of the Regulation.

According to Recital 31 DGA, data cooperatives seek to influence the terms and conditions of data user organisations attached to data use in a manner that

[52] Cf. Art. 2 (11) (c) and Recital 28 DGA.
[53] Cf. Recital 28 DGA.
[54] Cf. Recital 30 DGA.
[55] R Kulms, 'Data sharing and data protection' (2022) 1 Romanian Review of Private Law, 140.
[56] Understood as the unilateral act by which one person empowers another to represent him/her/them.
[57] E.g. Art. 1703 of the Italian Civil Code: «The mandate is the contract by which one party commits to perform one or more legal acts on behalf of the other».

gives better choices to the individual members of the group or potentially finding solutions to conflicting positions of individual members of a group on how data can be used where such data relates to several data subjects within that group, thus strengthening the position of individuals in making informed choices before consenting to data use.

Data cooperatives could also be useful for one-person undertakings and SMEs which, in terms of knowledge of data sharing, are often comparable to individuals.

Art. 2 (11) (b) and (d) DGA set out further exceptions to the applicability of the DGA: lett. (b) exempts intermediaries that focus on the intermediation of copyright-protected content, while lett. (d) applies to public-sector bodies that do not seek to establish commercial relationships.[58]

Finally, Art. 15 DGA deems its regime non-applicable to recognised data altruism organisations which do not establish commercial relationships.

Despite the definition regarding the concept of data intermediation the role of data intermediation services providers remains ambiguous: shaped as entities capable of securing the rights of data subjects in the technological context, they could instead end up enhancing the profitability of personal data encouraging its use for commercial purposes.[59] As it will be further discussed in section VI, this could lead to the reduction of the level of protection of personal data provided under EU law, implicating the debasement of fundamental rights.

4. Conditions for providing data intermediation services.

Art. 12 DGA imposes 15 conditions on data intermediation services.

Most obligations aim at protecting fair competition and ensuring a high level of security for users' data.

Art. 12 (a) DGA requires data intermediaries to refrain from using the data for which they provide data intermediation services for purposes other than to put them at the disposal of data users.

Providers of data intermediation services are prohibited from analysing and using the data shared by data holders for their own (or any other) purposes.[60]

Art. 12 (a) is further supplemented by Art. 12 (c) DGA, which prohibits the use of certain kinds of meta-data for other purposes than improving intermediation services.

Art. 12 (a) and (c) DGA by prohibiting providers of data information services to use both the data obtained from their users and the data collected by themselves to their users' disadvantage is aimed at avoiding conflicts of interest.[61]

The requirement of neutrality addresses concerns about vertically integrated platforms having a dual role by simultaneously acting as

[58] Cf. Recital 29 DGA.
[59] D Poletti, 'Gli intermediari dei dati' (2022) 1 European Journal of Privacy Law & Technologies, 53, https://doi.org/10.57230/EJPLT221DP.
[60] Cf. Recital 33 DGA.
[61] von Ditfurth, Lienemann, "The Data Governance Act' 283.

intermediary between businesses and users as well as competing with those businesses in offering their own services. An example is an undertaking that at the same time provides a marketplace where independent businesses can sell products to consumers and sells products as a retailer on the same marketplace in competition with the independent businesses. Such situations provide room for practices of self-preferencing, whereby a platform treats its own services more favourably than those of rivals.[62]

As mentioned, services providers may not use the data for other purposes than putting them at the disposal of their users. This implies that data intermediaries are generally not allowed to offer any additional data-related services to their users.

However, under Art. 12 (e) DGA data intermediaries may offer data-related services whose purpose it is to facilitate the exchange of data. For instance, data intermediation service providers can assist their users with the anonymisation of data.[63]

To make sure that data for which intermediation services are provided is not used for other purposes, Art. 12 (a) DGA imposes a requirement for the structural separation of data intermediation services from other units of the same company («the data intermediation services provider […] shall provide data intermediation services through a separate legal person»).

The structural separation should ensure that data or other insights gained from the provision of data intermediation services cannot be used for other activities pursued by the parent company or other affiliated firms.[64]

Art. 12 (b) DGA further prohibits providers from making the commercial terms, including pricing, for the provision of data intermediation services dependent on whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity.

Art. 12 (d) DGA requires providers of data intermediation services to conduct the exchange of the data in the format in which they receive it from a data subject or a data holder.

This should prevent service providers from imposing their own data standards on their users which could lead to the so-called "user lock-in".[65] However, the conversion of data formats is permitted if it improves interoperability, is requested by the parties to the data transaction, or is necessary to comply with international or European standards. In these instances, data holders and data subjects must be offered an opt-out option regarding the conversion. Alternatively, format conversion can be mandated by Union law: in those cases, data holders and data subjects cannot refuse conversion.

Relatedly, according to Art. 12 (i) DGA the services providers shall take appropriate measures to ensure interoperability with other data

[62] I Graef, R Gellert, 'The European Commission's proposed data governance act: Some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing' (2021) 006 TILEC Discussion Paper, 12, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3814721.
[63] Cf. Recital 32 DGA.
[64] von Ditfurth, Lienemann, 'The Data Governance Act' 284.
[65] ibid. 285.

intermediation services, i.e. by using common and open standards in the reference sector.

Additionally, common and open interoperability specifications will be promoted by the DA across sectors to achieve effective interoperability

between service providers. Arts. 33[66], 34[67] and 35[68] DA lay down the essential requirements and conditions to facilitate interoperability of data, data sharing

[66] Art. 33 DA « 1. Participants in data spaces that offer data or data services to other participants shall comply with the following essential requirements to facilitate the interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces which are purpose- or sector-specific or cross- sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives:
(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in a machine-readable format, to allow the recipient to find, access and use the data;
(b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, shall be described in a publicly available and consistent manner;
(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine- readable format where that is technically feasible and does not hamper the good functioning of the connected product;
(d) where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements, such as smart contracts shall be provided.
The requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements arising from other Union or national law.
2. The Commission is empowered to adopt delegated acts, in accordance with Article 45 of this Regulation to supplement this Regulation by further specifying the essential requirements laid down in paragraph 1 of this Article, in relation to those requirements that, by their nature, cannot produce the intended effect unless they are further specified in binding Union legal acts and in order to properly reflect technological and market developments.
The Commission shall when adopting delegated acts take into account the advice of the EDIB in accordance with Article 42, point (c)(iii).
3. The participants in data spaces that offer data or data services to other participants in data spaces which meet the harmonised standards or parts thereof, the references of which are published in the Official Journal of the European Union, shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards or parts thereof.
4. The Commission shall, pursuant to Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of this Article.
5. The Commission may, by means of implementing acts, adopt common specifications covering any or all of the essential requirements laid down in paragraph 1 where the following conditions have been fulfilled:
(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard that satisfies the essential requirements laid down in paragraph 1 of this Article and:
(i) the request has not been accepted;
(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or
(iii) the harmonised standards do not comply with the request; and
(b) no reference to harmonised standards covering the relevant essential requirements laid down in paragraph 1 of this Article is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).
6. Before preparing a draft implementing act referred to in paragraph 5 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation EU No 1025/2012 that it considers that the conditions in paragraph 5 of this Article have been fulfilled.
7. When preparing the draft implementing act referred to in paragraph 5, the Commission shall take into account the advice of the EDIB and views of other relevant bodies or expert groups and shall duly consult all relevant stakeholders.
8. The participants in data spaces that offer data or data services to other participants in data spaces that meet the common specifications established by implementing acts referred to in paragraph 5 or parts thereof shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such common specifications or parts thereof.

mechanisms, common European data spaces, as well as of interoperability of data processing services. Art. 36 DA also specifies some essential requirements for data sharing when using smart contracts.[69]

9. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. Where the reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the implementing acts referred to in paragraph 5 of this Article, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.
10. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraph 1, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.
11. The Commission may adopt guidelines taking into account the proposal of the EDIB in accordance with Article 30, point (h), of Regulation (EU) 2022/868 laying down interoperable frameworks for common standards and practices for the functioning of common European data spaces».

[67] Art. 34 DA «1. The requirements laid down in Article 23, Article 24, Article 25(2), points (a)(ii), (a)(iv), (e) and (f) and Article 30(2) to (5) shall also apply mutatis mutandis to providers of data processing services to facilitate interoperability for the purposes of in-parallel use of data processing services.
2. Where a data processing service is being used in parallel with another data processing service, the providers of data processing services may impose data egress charges, but only for the purpose of passing on egress costs incurred, without exceeding such costs».

[68] Art. 35 DA «1. Open interoperability specifications and harmonised standards for the interoperability of data processing services shall:
(a) achieve, where technically feasible, interoperability between different data processing services that cover the same service type;
(b) enhance portability of digital assets between different data processing services that cover the same service type;
(c) facilitate, where technically feasible, functional equivalence between different data processing services referred to in Article 30(1) that cover the same service type;
(d) not have an adverse impact on the security and integrity of data processing services and data;
(e) be designed in such a way so as to allow for technical advances and the inclusion of new functions and innovation in data processing services.
2. Open interoperability specifications and harmonised standards for the interoperability of data processing services shall adequately address:
(a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;
(b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;
(c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.
3. Open interoperability specifications shall comply with Annex II to Regulation (EU) No 1025/2012.
4. After taking into account relevant international and European standards and self- regulatory initiatives, the Commission may, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraphs 1 and 2 of this Article.
5. The Commission may, by means of implementing acts, adopt common specifications based on open interoperability specifications covering all of the essential requirements laid down in paragraphs 1 and 2.
6. When preparing the draft implementing act referred to in paragraph 5 of this Article, the Commission shall take into account the views of the relevant competent authorities referred to in Article 37(5), point (h) and other relevant bodies or expert groups and shall duly consult all relevant stakeholders
7. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraphs 1 and 2, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.
8. For the purpose of Article 30(3), the Commission shall, by means of implementing acts, publish the references of harmonised standards and common specifications for the interoperability of data processing services in a central Union standards repository for the interoperability of data processing services.
9. The implementing acts referred to in this Article shall be adopted in accordance with the examination procedure referred to in Article 46(2)».

[69] Art. 36 DA «1. The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context

of executing an agreement or part of it, to make data available shall ensure that those smart contracts comply with the following essential requirements of:
(a) robustness and access control, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;
(b) safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;
(c) data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);
(d) access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers; and
(e) consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.
2. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall perform a conformity assessment with a view to fulfilling the essential requirements laid down in paragraph 1 and, on the fulfilment of those requirements, issue an EU declaration of conformity.
3. By drawing up the EU declaration of conformity, the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall be responsible for compliance with the essential requirements laid down in paragraph 1.
4. A smart contract that meets the harmonised standards or the relevant parts thereof, the references of which are published in the Official Journal of the European Union, shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards or parts thereof.
5. The Commission shall, pursuant to Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of this Article.
6. The Commission may, by means of implementing acts, adopt common specifications covering any or all of the essential requirements laid down in paragraph 1 where the following conditions have been fulfilled:
(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard that satisfies the essential requirements laid down in paragraph 1 of this Article and:
(i) the request has not been accepted;
(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or
(iii) the harmonised standards do not comply with the request; and
(b) no reference to harmonised standards covering the relevant essential requirements laid down in paragraph 1 of this Article is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).
7. Before preparing a draft implementing act referred to in paragraph 6 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers that the conditions in paragraph 6 of this Article have been fulfilled.
8. When preparing the draft implementing act referred to in paragraph 6, the Commission shall take into account the advice of the EDIB and views of other relevant bodies or expert groups and shall duly consult all relevant stakeholders.
9. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available that meet the common specifications established by implementing acts referred to in paragraph 6 or parts thereof shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such common specifications or parts thereof.
10. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. Where the reference of a harmonised standard is published in the Official Journal of the European Union,

Data intermediaries are also required to adhere to procedures for access to their services that are fair, transparent and non-discriminatory to users, including with regards to prices and terms of service (Art. 12 (f) DGA).

Providers of data intermediation services are prohibited from treating their users differently without justification. The prohibition on discrimination should prevent possible distortions of competition and market foreclosures.

Bearing in mind both the platform operators' ability to exclude third party providers from their platforms or to otherwise disadvantage them,[70] Art. 12 (f) DGA addresses the "gatekeeper" position of data intermediation services providers, obliging them to ensure that the procedure for access to their service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service.

This provision protects the ability of users to use multiple data intermediation services offered by different providers simultaneously (multi-homing), since exclusivity clauses imposed by providers on their users should be considered as unfair.[71]

Conversely, to facilitate the access and sharing of relevant data for companies that do not qualify as gatekeepers, the DA introduces an unfairness test for B2B contract clauses on data sharing that have been imposed on SMEs. More precisely, para 4 and 5 of Art. 13 DA lists a number of clauses that are unfair or presumed to be unfair, and contrary to good faith and fair dealing.[72]

---

the Commission shall repeal the implementing acts referred to in paragraph 6 of this Article, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.

11. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraph 1, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question».

[70] Stigler Center, Stigler Committee on digital platforms: Final Report (2019), 74.

[71] von Ditfurth, Lienemann, 'The Data Governance Act' 286.

[72] Art. 13 (4) (5) DA «4. In particular, a contractual term shall be unfair for the purposes of paragraph 3, if its object or effect is to:

(a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;

(b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in the case of non-performance of contractual obligations, or the liability of the party that unilaterally imposed the term in the case of a breach of those obligations;

(c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any contractual term.

5. A contractual term shall be presumed to be unfair for the purposes of paragraph 3 if its object or effect is to:

(a) inappropriately limit remedies in the case of non-performance of contractual obligations or liability in the case of a breach of those obligations, or extend the liability of the enterprise upon whom the term has been unilaterally imposed;

(b) allow the party that unilaterally imposed the term to access and use the data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party, in particular when such data contain commercially sensitive data or are protected by trade secrets or by intellectual property rights;

(c) prevent the party upon whom the term has been unilaterally imposed from using the data provided or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in an adequate manner;

(d) prevent the party upon whom the term has been unilaterally imposed from terminating the agreement within a reasonable period;

As stated in Art. 12 (l) DGA, all necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data must be taken by data intermediaries. Moreover, for the storage and transmission of competitively sensitive information it should be ensured the highest level of security.

Pursuant to Art. 12 (j) DGA, services providers are required to put in place adequate technical, legal and organisational measures in order to prevent unlawful transfers of or access to non-personal data. In substance, intermediation services providers are obligated to monitor data transactions of their users for violations of laws and to prevent illegal data transactions: providers are to assume responsibilities as "first-line enforcers" of the law.[73]

By focusing on the adequacy of measures, the provision could be interpreted in the sense that it would be sufficient to implement mechanisms for reporting legal violations by third parties and procedures for the exclusion of users.[74]

In the event of an unauthorized transfer, access or use of the non-personal data shared the data intermediation services provider is obliged to inform data holders without delay (Art. 12 (k) DGA).

According to Art. 12 (g) DGA, providers of data intermediation services are also required to have in place procedures for preventing fraudulent or abusive practices. Thus, data intermediation services providers will have to check the reliability of the services of potential users.

If the intermediaries offer data sharing services for natural persons, there is an additional fiduciary duty towards individuals that the provider bears in order to act in the best interests of data subjects when facilitating the exercise of their rights. This includes advising data subjects on potential data uses and on standard terms and conditions attached to such uses (Art. 12 (m) DGA).

An important data subject's right whose use data sharing services can facilitate is the right to data portability.[75]

(e) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data provided or generated by that party during the period of the contract or within a reasonable period after the termination thereof;
(f) enable the party that unilaterally imposed the term to terminate the contract at unreasonably short notice, taking into consideration any reasonable possibility of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for so doing;
(g) enable the party that unilaterally imposed the term to substantially change the price specified in the contract or any other substantive condition related to the nature, format, quality or quantity of the data to be shared, where no valid reason and no right of the other party to terminate the contract in the case of such a change is specified in the contract.
Point (g) of the first subparagraph shall not affect terms by which the party that unilaterally imposed the term reserves the right to unilaterally change the terms of a contract of an indeterminate duration, provided that the contract specified a valid reason for such unilateral changes, that the party that unilaterally imposed the term is required to provide the other contracting party with reasonable notice of any such intended change, and that the other contracting party is free to terminate the contract at no cost in the case of a change».

[73] Graef, Gellert, 'The European Commission's proposed data governance act' 12.

[74] von Ditfurth, Lienemann, 'The Data Governance Act' 287.

[75] Art. 20 (4) GDPR. On this topic see S Troiano, 'Il diritto alla portabilità dei dati', in N Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, (Cedam, 2019), 197 ff.; E Pelino, 'Diritti dell'interessato', in C Bistolfi, (ed.), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, (Giuffrè Francis Lefrebvre, 2016), 246 ff.; I Graef, M Husovec and N Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19(6) German Law Journal, 1359 ff., https://research.tilburguniversity.edu/en/publications/data-portability-and-data-control-lessons-for-an-emerging-concept.; L Somaini, 'The right to data portability and user control: ambitions and limitations'

Scholars highlighted the "multifunctional value" of this right which is capable, on the one hand, of enhancing at maximum the data subject's control over his/her data, thus representing the fullest expression of the right to personal data protection in its positive projection, on the other hand, being a right that has its initial justification in the stimulation of the market and competition, the data portability right represents a propulsive force for the free circulation of data.[76]

In the DGA's framework, the data portability right seems enhancing more the latter aspect, so much so that it appears more functional to the control of data holders, than to that of data subjects.[77]

Furthermore, where data subjects are provided with tools for giving consent or permissions to process data made available by data holders, the intermediary is obliged to specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data (Art. 12 (n) DGA).

Art. 12 (h) provides in the event of the insolvency of the data intermediation services provider, imposing a reasonable continuity of the provision of data intermediation services. In addition, whenever the above-mentioned services ensure the storage of data, data holders and data users have the right to obtain access to, to transfer or to retrieve their data, and whenever such data intermediation services are provided between data subjects and data users, data subjects can exercise their rights.

It is unclear how data intermediaries are supposed to ensure the continuity of their services in the event of insolvency, considering that according to the insolvency laws of most Member States the legal authority to decide about the continuation of a business is transferred to a liquidator or insolvency administrator once insolvency proceedings have begun.[78]

Lastly, pursuant to art. 12 (o) DGA data intermediation services providers are obliged to maintain a log record of the data intermediation activity.

5. The enforcement mechanism.

Pursuant to Art. 13 (1) DGA each Member State is required to designate one or more authorities responsible for carrying out the notification procedure and enforcing the DGA's rules within their jurisdiction.

The DGA does not specify whether the national authority should have a particular expertise or mandate. It is up to Member States to decide whether their data protection, competition, consumer or even cybersecurity agency is best placed to implement the notification framework.[79]

(2018) 3 Rivista di diritto dei media, 164 ff., https://www.medialaws.eu/wp-content/uploads/2019/05/8.-Somaini.pdf.

[76] Troiano, 'Il diritto alla portabilità dei dati' 199 ff.

[77] Poletti, 'Gli intermediari dei dati' 55.

[78] von Ditfurth, Lienemann, 'The Data Governance Act' 290. For example, with regard to Italian insolvency law cf. Arts. 128-129 D.lgs. 12 January 2019, n. 14, ("Codice della crisi d'impresa e dell'insolvenza").

[79] For this remark on the DGA proposal, see Graef, Gellert, 'The European Commission's proposed data governance act' 8.

Providers of data intermediation services are required to submit a notification to the competent authority of the Member State in which they have their main establishment (Art. 11 (1) DGA).

This obligation also applies to data intermediaries which are not established in the EU as long as they offer their services within the EU. International data intermediaries are required to designate a legal representative in one of the Member States where they intend to offer their services (Art. 11 (3) DGA).

In such cases, the designation of a legal representative is deemed necessary given that such data intermediation services providers handle personal data as well as commercially confidential data, which entails the close monitoring of the compliance of data intermediation services providers with the DGA.[80]

Furthermore, the notification system is designed as a one-stop-shop: according to Art. 11 (5) DGA, data intermediaries are entitled to offer their services in all Member States once they have notified the competent authority.

It must be noted that it is not required that the providers of data intermediation services are to be approved by the competent authority before taking up their services. According to Art. 11 (4) DGA, they can begin offering their services as soon as they have submitted a notification to the competent authority. In any case, pursuant to Art. 11 (9) DGA they can request that the competent authority confirms their compliance with the conditions set out in Art. 11 and 12 DGA.

Once they have taken up their services, providers of data intermediation services are required to follow the conditions set out in Art. 12 DGA.

The competent authorities of the Member States monitor the providers' compliance with the notification procedures and the conditions for providing data intermediation services (Art. 14 (1) DGA). Thus, the DGA framework consists of compulsory notification with only ex-post monitoring of whether providers of data sharing services comply with the applicable requirements.

Since the legality of data intermediation services is not checked by the competent authorities before they are allowed to take up their services, the approach chosen by the European Commission could be less effective in building user trust than a system of ex-ante authorization: potential users of such services have to rely on the threat of sanctions to provide sufficient incentives for data intermediation services providers to comply with the rules of the DGA.[81].

6. Risks of data sharing and the limits of the DGA.

Scholars have expressed concerns about the adequacy of the DGA's framework to achieve its multiple objectives, both questioning its actual potential in terms of achieving a competitive data market and pointing out its inconsistency and even harmfulness in terms of protecting the fundamental rights of data subjects.

[80] Cf. Recital 42 DGA.
[81] von Ditfurth, Lienemann, 'The Data Governance Act' 281-282.

First of all, it appears to be a certain tension between the DGA's approach to protecting horizontal and vertical competition and its objective of promoting the scaling up of data intermediaries.

The strict obligations imposed on data intermediation services in order to protect competition could turn out to severely limit the potential value of data sharing. More precisely, by vertically unbundling data intermediation services from other data related services and restricting the use of data generated by data intermediaries (Art. 12 (a) and (c) DGA), the DGA restrains their ability to capture economies of scope. [82] In other words, data intermediaries are prohibited from combining data generated by different services in order to gain valuable insights that could raise the quality of their data intermediation services.

Due to its rigidity, the framework of the DGA prohibits practices without exceptions, even if they are procompetitive and efficient to the development of the EU data economy, thus reducing the value data intermediation services can provide to their users.[83]

Furthermore, the strict obligations aimed at protecting competition will increase the already considerable regulatory burdens faced by data intermediaries. They could also, in some instances, prevent pro-competitive and desirable activities by non-dominant data intermediaries and cut off the market's process of experimentation at a time when few data intermediaries have been established successfully.[84] In this respect, it must be noted that the addressee of the DGA are companies that are young and are yet to develop a relevant market power.

The scope and intensity of the DGA's framework can be compared to that of the Digital Markets Act.[85] However, it should be pointed out the different circumstances in the respective industries: while the industries targeted by the Digital Markets Act are quite concentrated and mainly consist of a few large US-based players, the data sharing services the DGA wishes to promote are still mostly in their infancy.[86]

With regard to the compatibility between the DGA and the instance of protecting data subjects' personal data from external aggression, it seems that the new Regulation reproduces the issues regarding the conflict between facilitating the mass transfer of personal data through interoperable formats or otherwise, allowing for the easy and rapid reuse of such data, and the principle of data minimization set forth in Art. 5 (1) (c) GDPR.[87]

The promotion of data sharing seems to hopelessly conflict with the underlying spirit of the other rights of the data subject, namely the need for minimization of data and related risks to processing of personal data.

In the DGA's framework data subjects' rights seem to be inextricably linked to the stimulation of the market and competition. According to the new

[82] ibid. 289.
[83] ibid.
[84] ibid. 292. See also G Resta, 'Pubblico, privato, collettivo nel sistema europeo di governo dei dati' (2022) 4 Rivista trimestrale di diritto pubblico, 990.
[85] J Baloup and others, 'White paper on the data governance act' (2021), 32, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703.
[86] Graef, Gellert, 'The European Commission's proposed data governance act' 11.
[87] See Troiano, 'Il diritto alla portabilità dei dati' 210-211 ff. on the data portability right.

Regulation, fundamental rights appear more functional to the commercial activity carried out by intermediaries and data holders, than to the protection of data subjects.

The DGA constitutes yet another confirmation of a new way of interpreting personal data protection law, whose personalistic principle gradually gives way to the need to promote the free movement of personal data.[88]

Conclusions.

The regulatory approach chosen for the DGA, on the one hand, could keep data intermediation services from fully unlocking their potential as much-needed matchmakers on markets for data sharing, on the other hand, carries a tension between data protection principles and data sharing, as reported by the EDPB and the EDPS in their joint opinion.

With regard to this last aspect, it is undisputed that the coordination between the DGA and the GDPR requires going beyond general and abstract phrasing such as the one contained in Art. 1 (3) DGA, according to which «this Regulation is without prejudice to Regulation (EU) 2016/679 […]».

In general, the counterweights provided by the DGA do not seem sufficient to contain the risks of the commodification of personal data entailed in data intermediation services, due to their vagueness and difficult application.

At present, the compatibility of the DGA with the rest of the EU acquis looks like a mere afterthought that is left to market players to figure out.[89] If anything, to make sure the DGA achieves its objectives, compliance with the EU data protection law should have been considered upfront, during the legislative process. Only in doing so it would have been possible to offer a (consciously) positive answer to the question posed by this paper: does sharing mean caring?

[88] According to N Zorzi Galgano, 'Le due anime del GDPR e la tutela del diritto alla *privacy*', in N Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, (Cedam, 2019), 36 ff., two fundamental rights emerge from the GDPR, two souls that constitute an explication of the protection provided therein, on the one hand, the so-called right to privacy of the data subject, and on the other hand, the right to data processing and the right to data circulation, both manifestation of freedom to conduct a business.

[89] See, on the DGA proposal Graef, Gellert, 'The European Commission's proposed data governance act' 15.

Lombardi A, 'Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra GDPR e AI Act' (2023) 2 EJPLT, 240 - 252.
DOI: https://doi.org/10.57230/EJPLT232AL

EJPLT
ISSN 2704-8012



Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra *GDPR* e *AI Act*

Data protection regulation and artificial intelligence regulation: relationships, similarities and differences between GDPR and AI Act

ANTONGIULIO LOMBARDI
Esperto di diritto e tecnologia

Abstract

La convergenza, sotto plurimi profili, tra la normativa in materia di protezione dei dati personali e quella, *in fieri*, relativa alle applicazioni dell'intelligenza artificiale (*AI*) sta emergendo in modo tangibile. Il contributo si propone, pertanto, di sinteticamente esaminare i principali punti di contatto e le divergenze tra GDPR e (proposta di) Regolamento per un *Artificial Intelligence Act*.

The convergence, in many respects, between the laws on protection of personal data and the rules, in progress, relating to the applications of artificial intelligence (AI) is emerging in a tangible way. The contribution aims to briefly examine the main points of contact and divergences between the GDPR and the (proposal for) Regulation for an Artificial Intelligence Act.

© The author(s) 2023, 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: Protezione dei dati; Artificial Intelligence Act; Consenso; Trasparenza; Regolamento UE 2016/679.

Summary: 1. Origini, finalità e principi sottesi alla disciplina della tutela dei dati personali e alla regolamentazione dell'AI. – 2. Riferimenti applicabili all'AI nel GDPR. – 3. Analogie e differenze tra le due discipline. – 3.1. I doveri di trasparenza – 3.2. Correttezza e accuratezza dei dati – 4. Le modifiche allo schema di AI Act nel testo approvato il 14 giugno 2023, nell'ottica di un implementato coordinamento con il GDPR. – 5. Conclusioni.

1. Origini, finalità e principi sottesi alla disciplina della tutela dei dati personali e alla regolamentazione dell'AI.

La convergenza tra la normativa in materia di protezione dei dati personali e quella, *in fieri*, relativa alle applicazioni dell'intelligenza artificiale (*AI*) sta emergendo in modo tangibile. Le discipline – i cui oggetti e scopi possono apparire, *prima facie*, profondamente differenti (bilanciamento tra diritti dell'individuo quanto alla gestione dei propri dati e promozione della loro circolazione, l'una[1]; lo sviluppo responsabile di sistemi di *AI*, nell'ottica di una minimizzazione dei connessi rischi per gli individui, l'altra[2]) – sono connotate da finalità comuni, e da ambiti applicativi talora (quantomeno parzialmente) coincidenti, come nel prosieguo si illustrerà.

Presupposto dell'analisi che si intende sviluppare è, come è ovvio, la strutturale differenza tra le due discipline e le relative finalità, che riflette, del resto, la diversità dei diritti e degli interessi che la normativa sui dati personali (il GDPR, principalmente) e il (la proposta di) Regolamento per un *Artificial Intelligence Act* sono rispettivamente volti a tutelare, e, in ultima istanza, la diversa natura delle due normative. Non è certo questa la sede per compiutamente esaminare tali plurime differenze, né certo per soffermarci sulla disamina dei diritti (fondamentali) alla cui protezione le due normative sono volte.

Su un primo, e più superficiale, livello, infatti, occorre evidenziare che, da un lato, l'*Artificial Intelligence Act*, per quanto di elevato impatto su un'ampia serie di diritti fondamentali dell'individuo, oltre che di interessi generali "della collettività", pare destinato a iscriversi nel novero di norme che, nel diritto

Si ringrazia per la collaborazione Antonio Lombardi e Giulio Lombardi.

[1] Cfr. art. 1 Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

[2] Cfr. Proposta di Regolamento per un *Artificial Intelligence Act* della Commissione UE del 21 aprile 2021. Nel prosieguo si farà riferimento in particolare alla versione della proposta di Regolamento emergente a fronte delle modifiche apportate dal Parlamento europeo, e dunque alla versione del 14 giugno 2023, non essendo, al momento della redazione del presente scritto, ancora disponibile la versione emendata a seguito del trilogo del dicembre 2023. Si fa, in particolar modo, riferimento qui all'*Amendment* 140 (*Article* 1 – *paragraph* 1: "*The purpose of this Regulation is to promote the uptake of human-centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and the rule of law, and the environment from harmful effects of artificial intelligence systems in the Union while supporting innovation*").

unionale, compongono l'ambito della *product safety*, o comunque di quelle norme volte a regolare, *ex ante*, la produzione di particolari "beni" (e non ci addentriamo qui nella articolata tematica della qualificabilità del sistema di A.I. come "prodotto" oppure come "servizio") in aderenza a determinati standard di fabbricazione, controllo e monitoraggio (sia *pre-* che *post-market*). Come la stessa proposta della Commissione riconosce, infatti, il Regolamento dovrà integrarsi con la già esistente normativa, orizzontale e verticale, in materia di sicurezza dei prodotti. Per converso, la natura del GDPR è sicuramente differente, trattandosi di previsioni che disciplinano il diverso settore del trattamento dei dati personali.

Su un ulteriore piano, inoltre, se il GDPR si propone di tutelare diritti fondamentali come la protezione dei dati personali e dell'identità personale, le regole che l'*Artificial Intelligence Act* mira a introdurre non esauriscono certo le proprie finalità nella tutela del solo diritto alla protezione dei dati, essendo finalizzato alle protezione di un novero ben più ampio di diritti fondamentali dell'individuo (eguaglianza, non discriminazione, salute…), oltre che della "collettività" (si pensi, a titolo meramente esemplificativo, all'impatto dell'*AI* sul corretto funzionamento delle istituzioni democratiche).

Pur avendo ben chiare tali strutturali differenze tra le due normative, si ritiene comunque indispensabile effettuarne una lettura combinata e integrata, al fine di evidenziare non soltanto eventuali "lacune" o esigenze di più stretta correlazione, ma altresì

Ma procediamo con ordine, prendendo le mosse da una (sintetica) disamina delle finalità che a chi scrive paiono connotare entrambe le normative:

a. Esigenza di diffusione e circolazione dei dati

Si tratta della necessità di consentire una diffusione efficiente e sicura dei dati, senza frapporre ostacoli ingiustificati alla loro libera circolazione tra le parti interessate. La disciplina sulla protezione dei dati personali si concentra sulla gestione appropriata di queste informazioni, funzionale a garantire sia la *privacy* (non è certo questa la sede per tornare sulle note differenze tra diritto alla riservatezza e diritto alla protezione dei propri dati personali), sia la sicurezza degli individui. A tal riguardo, la regolamentazione dell'*AI* (si fa riferimento principalmente alla proposta di *Artificial Intelligence Act – AI Act* varata dalla Commissione UE nell'aprile 2021, approvata con modifiche dal Parlamento europeo nel giugno 2023, e della quale si attende l'approvazione definitiva dei prossimi mesi) mira a creare un ambiente in cui i dati possano alimentare e migliorare lo sviluppo di sistemi di *AI*: i dati, come è noto, costituiscono il motore principale dell'evoluzione di tale tecnologia.

Quanto all'ambito della *data protection*, la promozione della circolazione dei dati è tratto comune non soltanto del GDPR, ma altresì – e ancor più – di altre norme unionali, quali in particolare il *Data Governance Act* (Regolamento 2022/868).

b. Necessità di tutela dell'interesse dell'individuo

Si fa riferimento alla necessità di proteggere gli interessi, i diritti e le libertà degli individui, in un contesto in cui i dati personali e i sistemi di *AI* sono ampiamente utilizzati. La disciplina di *data protection* si preoccupa di garantire

che i singoli (persone fisiche) mantengano il controllo sui dati che li riguardano e che siano protette da abusi, discriminazioni o violazioni della *privacy*. Allo stesso modo, la regolamentazione dell'*AI*, in particolar modo basata sulla previsione di specifiche categorie di rischio e sulla conseguente modulazione dei relativi requisiti regolatori, tenta di minimizzare i rischi derivanti dall'uso di tali sistemi al fine di garantire che le decisioni automatizzate non danneggino gli individui, o "la società" nel suo complesso.

In definitiva, sebbene la protezione dei dati personali e la regolamentazione sull'*AI* possano sembrare divergenti nelle loro origini storiche e nelle apparenti finalità, in realtà convergono nell'obiettivo comune di creare un ambiente in cui i dati possano circolare in modo sicuro ed efficiente, preservando al contempo l'interesse e la dignità degli individui e lo sviluppo tecnologico.

Mette conto di sottolineare che la regolamentazione della protezione dei dati personali ha attraversato un complesso processo di creazione ed evoluzione, sviluppatosi per oltre un secolo, nel corso del quale lo stesso concetto di "dati personali" ha subito una evoluzione che, prendendo le mosse dal concetto di "*privacy* individuale" (la cui nascita è tradizionalmente imputata al noto articolo di Warren e Brandeis[3]) giungendo sino alla differente nozione di protezione dei dati, il cui flusso ha rilevante impatto sociale e interesse generale.

Al contrario, la regolamentazione relativa all'uso dei sistemi di *AI* è emersa solo negli ultimi dieci anni ed è ancora in fase di sviluppo, non esistendo ad oggi un definitivo quadro normativo generale né nell'Unione Europea né negli Stati Uniti d'America; mentre una eccezione degna di nota è rappresentata dalla Repubblica Popolare Cinese[4], che ha recentemente introdotto disposizioni vincolanti specifiche per i sistemi di *AI* generativa.

Occorre inoltre osservare che l'evoluzione delle norme di cui alla proposta di *AI Act*, con gli emendamenti formulati solo nel dicembre 2022[5], ha rappresentato un primo passo verso la regolamentazione dei *deepfake*[6] e dell'*AI* generativa[7]. Il che dimostra, tra l'altro, quanto sia complesso definire regole suscettibili di essere applicate nel lungo periodo per adeguarsi alla costante evoluzione dell'*AI*.

La disciplina per la protezione dei dati personali ha seguito un percorso parallelo all'aumento dell'utilizzo e dello scambio di dati, pur talora faticando a "tenere il passo" con l'evoluzione tecnologica (sono note le critiche da più parti mosse, al riguardo, al GDPR).

Questo argomento non può essere applicato in modo simile ai sistemi di *AI* che attualmente contano miliardi di utilizzatori in tutto il mondo, operando in assenza di un quadro normativo definito, quando solo una limitata parte degli

---

[3] S.D Warren, L.D Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, 5, 193 ss. (in JSTOR, https://doi.org/10.2307/1321160). Tale articolo citato contiene suggestioni che, all'occhio del lettore contemporaneo, appaiono quasi profetiche quanto alla configurazione delle problematiche tipiche dell'*AI*, come il riferimento alle "*recent inventions*" riferito alla (allora recente) fotografia riprodotta nell'articolo medesimo.

[4] Cfr. Le *Interim Measures for the management of generative Artificial intelligence services* (in http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm).

[5] https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

[6] Emendamenti 101, 102, 399.

[7] Emendamenti 203, 486, 487.

utenti è consapevole della loro presenza e funzionamento.

In un tale contesto, possiamo affermare in termini generali che, sebbene il consenso informato e volontario dell'individuo possa talora rivelarsi uno strumento efficace per risolvere parte delle questioni legate alla protezione dei dati personali (pur consapevoli delle plurime criticità che la più accorta dottrina da tempo rileva), esso si dimostra inadeguato nel caso della regolamentazione dei sistemi di *AI*. Questi sistemi, data la loro pervasività in una vasta gamma di applicazioni, inevitabilmente superano gli interessi e le conoscenze individuali, rendendo il consenso dell'individuo inefficace nel dirimere le connesse problematiche.

2. Riferimenti applicabili all'AI nel GDPR.

Come noto, l'art. 22 del GDPR concerne le decisioni assunte sulla base di trattamenti automatizzati di dati personali operati da sistemi che utilizzano algoritmi. A tal proposito possiamo enucleare tre principi fondamentali:

a. Consapevolezza (o conoscibilità) e comprensione

Si tratta del diritto dell'individuo di essere messo a conoscenza della presenza o meno di processi automatizzati che lo riguardino, e quindi di ricevere informazioni significative sulla modalità di attuazione di detti processi, anche con riguardo alla logica sulla quale essi si fondano. Tale principio si scontra con una difficoltà non tanto connessa alla protezione del diritto di proprietà intellettuale dell'algoritmo utilizzato, quanto agli obiettivi e spesso ineliminabili limiti dell'esser umano, nella maggior parte dei casi, nel comprendere la modalità "tecniche" di funzionamento dell'algoritmo stesso.

b. Non esclusività o verifica umana

Se una decisione automatizzata produce effetti giuridici che riguardano o che incidano significativamente su una persona, detta decisione non deve essere fondata solo sul processo automatizzato ma necessita di un controllo e di una valutazione di un umano (in grado di essere) *in command*. Tale principio si esplica in concreto, da una parte, nella supervisione dell'uomo sugli utilizzi dell'*AI* e, dall'altra, nell'impiego dell'*AI* come una delle possibili origini degli elementi posti alla base della scelta dell'uomo, ma mai l'unica[8].

Va rammentato che per il GDPR una decisione algoritmica può validamente e legittimamente avere effetto sui diritti di un individuo in una serie di casi che, per vero, per la loro evidente ampia possibilità di verificarsi, costituiscono ben più di mere "eccezioni alla regola": i) quando vi sia il consenso esplicito dell'interessato; ii) quando l'utilizzo di strumenti automatizzati sia necessario per concludere o eseguire un contratto tra interessato e titolare del trattamento; iii) quando tale utilizzo sia autorizzato dal diritto dell'Unione o dello stato membro.

[8] Nell' *HITL (human-in-the-loop)* per produrre il risultato è necessario che la macchina interagisca con l'essere umano. Cfr. V. S. Bisen *What is Human in the Loop Machine Learning: Why & How Used in AI?*, 20 maggio 2020.

c. Non discriminazione[9]

Le conclusioni o "decisioni" formulate dall'algoritmo non devono avere effetti discriminatori. Tale prescrizione prescinde in gran parte da quanto detto sopra sulla conoscibilità del funzionamento algoritmico e sul controllo e supervisione da parte dell'essere umano: semplicemente, ove i dati immessi nel sistema di decisione automatizzata (dati di *input*) siano erronei, erroneo sarà altresì l'*output* prodotto dal sistema[10].

3. Analogie e differenze tra le due discipline.

Pur consci delle diversità tratteggiate *retro*, è indiscusso che il GDPR e l'attuale versione dell'*AI Act* presentino numerosi elementi in comune. La struttura è sostanzialmente analoga: le due materie trovano nei regolamenti una disciplina completa e organica sia nel merito che quanto all'apparato sanzionatorio.

Entrambi i documenti sono una chiara espressione del primato normativo dell'Unione Europea, e della opzione di *policy* consistente nel non lasciare al solo funzionamento del mercato la disciplina di settori cruciali, sopperendo alle esigenze normative con discipline esaustive e complete, per quanto possibile al momento dell'approvazione (analoga opzione legislativa è stata seguita nella materia delle comunicazioni elettroniche).

Il fenomeno, appena percepibile nel GDPR, di non perfetto allineamento tra disposto normativo ed esigenze concrete presenti al momento della prima applicazione, risulta nella proposta di *AI Act* estremamente chiaro; tanto che, considerando l'evoluzione dei sistemi di *AI*, è certo che al momento della effettiva applicazione dell'*AI Act* emergeranno aspetti non marginali che necessiteranno di allineamenti o di ulteriore disciplina (o di modifica di quella varata).

Diversi aspetti necessitano di particolare attenzione e di diversa disciplina nei due ambiti in considerazione: da una parte, il consenso dell'interessato, che può essere non sufficiente nei casi di impiego di *AI* (suscettibili di avere significativo impatto anche su soggetti terzi, che non esprimono alcun consenso); dall'altra, l'osservazione secondo la quale la consapevolezza di stare interagendo con un sistema di *AI*, che deve essere assicurata prima che

[9] Cfr. considerando n. 71 del GDPR: "*tenendo in considerazione le circostanze ed il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori [enfasi aggiunta] e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni per-sonali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti*".

[10] È il principio noto come GIGO– "*garbage in garbage out*" – in virtù del quale un algoritmo riflette la qualità dei dati da cui è alimentato (si pensi al noto "caso Compas" negli Stati Uniti). Cfr. F LAGIOIA., R. ROVATTI, G SARTOR. *Algorithmic fairness through group parities? The case of COMPAS-SAPMOC. AI & Soc* 38, 459–478 (2023). https://doi.org/10.1007/s00146-022-01441-y

l'umano sia posto di fronte all'impiego della stessa, non essendo evidentemente idonea una informativa tardiva, che intervenga in un momento nel quale la "relazione" tra umano e *AI* si sia già instaurata.

3.1. I doveri di trasparenza

Il tema può essere anche descritto in termini più generali come comportante l'esigenza di un diverso concetto di "trasparenza" nell'applicazione delle norme di cui alla proposta di *AI Act* rispetto a quello sul quale si fonda l'operatività del GDPR. In particolare:

- nel GDPR le prescrizioni di trasparenza sono oggetto, oltre che dei considerando 39, 58 e 60, dell'art. 5.1 a) e dell'art. 12, prevedendo una serie di attività che il titolare del trattamento deve attuare per rendere noto agli interessati non solo l'esistenza del trattamento di loro dati personali, ma anche i relativi effetti;
- nella proposta di Regolamento sull'*AI*, la "trasparenza" trova menzione in quello che è oggi l'art. 4-*bis*, lettera d), che prevede al riguardo che: "*i sistemi di AI sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di AI e informando debitamente gli utenti delle capacità e dei limiti di tale sistema di AI e le persone interessate dei loro diritti*".

Rammentiamo altresì la portata dell'art. 13 dell'*AI Act* (nella ultima versione del 14 giugno 2023), ove si prevede che i sistemi di *AI* ad alto rischio devono essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai fornitori e agli utenti di comprendere ragionevolmente il funzionamento del sistema. Dovrebbe essere così garantito un livello di trasparenza adeguato in conformità della finalità prevista per l'impiego del sistema di *AI*, che consenta di conseguire il rispetto dei pertinenti obblighi del fornitore e dell'utente di cui al capo III. Il testo del 14 giugno 2023 ha esteso i doveri di trasparenza anche ai fornitori di sistemi di *AI*, contemplando la necessità che sia garantita una ragionevole comprensione del funzionamento del sistema di *AI* in conformità alle relative finalità.

Le prescrizioni di "trasparenza" si traducono, pertanto, nell'esigenza che, al momento dell'immissione sul mercato del sistema di *AI* ad alto rischio, siano utilizzati tutti i mezzi tecnici disponibili, conformemente allo stato dell'arte generalmente riconosciuto, per garantire che l'*output* del sistema di *AI* sia interpretabile dal fornitore e dall'utente. L'utente deve essere in grado di comprendere e utilizzare adeguatamente il sistema di *AI*, sulla base di una conoscenza generale del suo funzionamento e dei dati trattati; il che gli consentirebbe di adeguatamente "spiegare" le decisioni adottate dal sistema di *AI* alla persona interessata a norma dell'art. 68, lettera c).

Nel Titolo IV (ora rubricato "*Obblighi di trasparenza*", essendo stata rimossa la specificazione "*per determinati sistemi di AI*"), l'art. 52.1 prevede il dovere dei fornitori di garantire che i sistemi di *AI* destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che il sistema di *AI*, "*il fornitore stesso o l'utente informino in modo tempestivo, chiaro e*

comprensibile la persona fisica esposta a un sistema di AI del fatto di stare interagendo con un sistema di AI, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo".

L'art. 52.3, poi, pur non menzionando espressamente la parola "trasparenza", ne fornisce una chiara modalità di applicazione con riguardo a sistemi di *deepfake* (tema originariamente solo accennato nel testo dell'aprile 2021), prevedendo che gli utenti di un sistema di *AI* che genera o manipola testi o contenuti audio o visivi che potrebbero apparire falsamente autentici o veritieri, e che rappresentano persone che sembrano affermare cose che in verità non hanno mai affermato o compiere azioni che non hanno mai posto in essere, senza il consenso delle persone stesse, sono tenuti a rendere noto in modo adeguato, tempestivo, chiaro e visibile i) che il contenuto è stato generato o manipolato artificialmente e ii) il nome della persona fisica o giuridica che li ha generati o manipolati.

A tal fine, i contenuti sono "etichettati" in modo da segnalare il loro carattere non autentico in maniera chiaramente visibile alle persone cui sono destinati. Tanto, tenendo conto dello stato dell'arte generalmente riconosciuto e delle pertinenti norme e specifiche tecniche armonizzate.

La proposta di *AI Act* delinea doveri di trasparenza generali, suscettibili di trovare applicazione anche in assenza di trattamento di dati personali. Inoltre, produttore, fornitore e utente di sistemi di *AI* è soggetto, al riguardo, a doveri differenti rispetto a quelli al cui rispetto è tenuto il titolare del trattamento dei dati personali (a prescindere dall'impiego o meno, da parte dello stesso, di applicazioni di *AI*).

In particolare, fornitori e utenti di sistemi di *AI* sono soggetti alle norme del GDPR soltanto se qualificabili altresì come "titolari" o "responsabili" del trattamento di dati personali, essendo a questi ultimi che il Regolamento UE eminentemente si rivolge. Inoltre, in materia di *AI*, l'art. 22 del GDPR trova applicazione unicamente nei casi di impiego di sistemi di *AI* che attuano decisioni automatizzate o pongono in essere attività qualificabili come profilazione di individui, potendo rimanere esterni all'ambito applicativo della norma non pochi sistemi "intelligenti" (si pensi, ad esempio, ai più semplici *chatbot*).

Tanto premesso, venendo alle informazioni da fornire e alla loro finalità, si osserva quanto segue:

- ai sensi del GDPR, le informazioni hanno la finalità di rendere consapevoli gli interessati dei rischi connessi al trattamento e delle relative conseguenze, nonché, nel caso di profilazione ai sensi dell'art. 22, la logica cui risponde il trattamento automatizzato (cfr. art. 13.2, lett. f, nonché considerando 63 del GDPR);
- per la proposta di *AI Act*, le informazioni da trasmettere sono quelle espressamente previste dall'art. 52, ossia: i) il "*fatto di stare interagendo con* [un sistema di *AI*, n.d.r.] *a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo*"; ii) per sistemi che generano *deepfake*, "*il contenuto che è stato generato o manipolato*"; iii) per sistemi non vietati di "*riconoscimento delle emozioni*" o di "*categorizzazione biometrica*", il "*funzionamento del sistema*".

A ciò si aggiunga che l'art. 13.3, lett. b) dell'*AI Act* stabilisce l'obbligo di

fornire agli utenti istruzioni comprensibili in formato digitale che contengano informazioni rilevanti sulle azioni dell'utente che possono avere un impatto sulle prestazioni del sistema di *AI*. Si tratta di informazioni riguardanti la tipologia e la qualità dei dati di *input* elaborati, così come qualsiasi altra informazione rilevante riguardo ai *set* di dati utilizzati per l'addestramento, la convalida e le prove del sistema.

3.2. Correttezza e accuratezza dei dati

Nell'impianto del GDPR il tema della correttezza e accuratezza dei dati[11] riceve disciplina:

- nell'art. 15.1, lett. d) ("*Principi applicabili al trattamento di dati personali*"), secondo il quale i dati personali devono essere esatti e, ove necessario, aggiornati, prescrivendo altresì il dovere di adottare ogni misura ragionevole per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- nell'art. 18.1, lett. a) ("*Diritto di limitazione di trattamento*"), a norma del quale l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando, tra l'altro, si contesti l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificarne la correttezza.

La centralità del principio di esattezza dei dati risulta evidente, poi, anche ai fini di una effettiva applicazione dell'art. 22 del GDPR, essendo la correttezza dei dati elaborati indispensabile al fine di prevenire che il loro trattamento automatizzato produca esiti distorti o non rispondenti al vero.

Il tema dell'esattezza dei dati trova, poi, trattazione specifica nell'*AI Act*, anche sull'assunto che una eccessiva accuratezza dei dati, ove ottenuta a scapito delle esigenze di riservatezza individuale e ponendo in essere indagini *A.I.-powered* smodatamente penetranti, può condurre ad eccessiva invasività nella sfera personale. Al riguardo, il considerando 50 della proposta di *AI Act* afferma che "*gli utenti del sistema di AI dovrebbero adottare misure per garantire che il possibile compromesso tra robustezza e accuratezza non produca risultati discriminatori o negativi per sottogruppi minoritari*".

In particolare, il testo della proposta di Regolamento approvato il 14 giugno 2023 tocca il tema dell'esattezza dei dati:

- all'art. 15.1, secondo il quale i sistemi di *AI* ad alto rischio devono essere progettati e sviluppati in aderenza al principio della sicurezza fin dalla progettazione (*by design*) e per impostazione predefinita (*by default*), anche al fine di garantire un "*adeguato livello di accuratezza*", mediante l'adozione di misure conformi allo stato dell'arte, secondo lo specifico segmento di mercato o campo di applicazione;
- all'art. 2, ove si prevede che i livelli di accuratezza e le pertinenti metriche di accuratezza dei sistemi di *AI* ad alto rischio sono dichiarati nelle istruzioni per l'uso che accompagnano il sistema.
- al considerando 44, ove si riconosce il ruolo cruciale dell'accesso a dati di alta qualità nel garantire il corretto funzionamento e la sicurezza dei

[11] Il tema è stato oggetto di analisi approfondita nel corso delle audizioni consultive svolte dalle commissioni parlamentari nel 2022.

sistemi di *AI* ad alto rischio, prevenendo così la discriminazione. I *set* di dati di addestramento e validazione dei sistemi (convalida e prova) dovrebbero, dunque, essere sufficientemente pertinenti, rappresentativi, adeguatamente verificati in termini di errori e il più possibile completi in base agli scopi previsti, oltre a essere caratterizzati da adeguate proprietà statistiche, anche al fine di prevenire distorsioni che potrebbero minacciare i diritti fondamentali o produrre risultati discriminatori.

Con specifico riguardo, poi, alle attività poste in essere da autorità di contrasto implicanti l'utilizzo di sistemi di *AI*, il considerando 38 della proposta di Regolamento riconosce come l'impiego di tali sistemi in siffatti contesti possa condurre a esiti discriminatori o ingiusti di particolare gravità, *inter alia*, ove gli stessi non vengano addestrati con dati di elevata qualità, e dunque di qualificata accuratezza. Il caso dell'impiego dell'*AI* per attività quali quelle di controllo ed *enforcement* dell'autorità giudiziaria, ma anche nel più ampio settore della giustizia, costituisce esempio particolarmente illustrativo della centralità dell'esigenza di accuratezza dei dati elaborati dall'A.I., in considerazione dell'incidenza su diritti fondamentali della persona.

La qual cosa solleva altresì articolate questioni concernenti la necessità di garantire idonei livelli di trasparenza e spiegabilità dei sistemi in questione (in relazione ai quali pare, dunque, da condividere la scelta di classificazione come "ad alto rischio"). Peraltro, solo in presenza di idonee caratteristiche di trasparenza sarà possibile verificare l'esattezza dei dati elaborati dall'*AI*, anche al fine di contestarne gli *output* in sede giudiziale.

Lo stesso dicasi, ad esempio, anche per impieghi dell'*AI* nella gestione della migrazione, dell'asilo e del controllo delle frontiere (considerando 39), o in ambito sanitario, anche in relazione alla particolare vulnerabilità dei soggetti interessati in entrambi i casi.

4. Le modifiche allo schema di AI Act nel testo approvato il 14 giugno 2023, nell'ottica di un implementato coordinamento con il GDPR

L'*iter* legislativo seguito dalla proposta di *AI Act* (secondo lo schema del trilogo) ha consentito un graduale adeguamento delle disposizioni in esame anche ai mutamenti del contesto di fatto e tecnologico, oltre a un riallineamento delle disposizioni della proposta al fine di garantire un (inizialmente non sufficiente) coordinamento con il GDPR. Obiettivo, questo, che pare essere stato raggiunto dal testo approvato dal Parlamento europeo il 14 giugno 2023.

I rimandi al *GDPR* nella ultima versione del testo della proposta di Regolamento sono numerosi. In questa sede ci si limita a ricordare, nell'ordine, le seguenti disposizioni, introdotte nel testo approvato nel giugno 2023:

- considerando 15: si riconosce il rischio di utilizzo improprio dell'*AI* per pratiche di manipolazione, sfruttamento e controllo sociale che contraddicono i "valori" dell'Unione, tra cui il diritto alla non discriminazione, alla protezione dei dati e alla vita privata;

- considerando 28-*bis*: nella valutazione dell'impatto negativo dei sistemi di *AI* sui diritti fondamentali protetti dalla Carta dei diritti fondamentali dell'Unione europea, specialmente ai fini della classificazione di un determinato sistema come "ad alto rischio", occorre porre mente anche al diritto alla protezione dei dati personali;
- considerando 33-*bis*: anche in considerazione della particolare tutela accordata dal GDPR, si propone la classificazione come "ad alto rischio" dei sistemi di *AI* destinati all'identificazione delle persone fisiche o all'analisi delle loro caratteristiche personali basate su dati biometrici o elementi biometrici, escludendo i sistemi di verifica biometrica che confermano l'identità di una persona per l'accesso a servizi o dispositivi;
- considerando 41-*bis*: si chiarisce l'applicabilità di norme vigenti a livello europeo (ma anche nazionale e internazionale) anche ai sistemi di AI, tra cui le norme in materia di *data protection*;
- considerando 45-*bis*: il diritto alla vita privata e alla protezione dei dati personali deve essere garantito durante tutto il ciclo di vita del sistema di *AI*, con particolare enfasi su principi quali quello di minimizzazione dei dati e di loro protezione fin dalla fase di progettazione e per impostazione predefinita, oltre a prescrivere l'adozione di misure tecniche e organizzative avanzate per proteggere i diritti fondamentali, compresa l'anonimizzazione, la cifratura e l'uso di tecnologie che consentono l'elaborazione di dati senza la loro trasmissione tra le parti, ove superflua;
- art. 2, par. 5-*bis*: stabilisce che il diritto dell'Unione in materia di protezione dei dati personali, vita privata e riservatezza delle comunicazioni si applica ai trattamenti di dati personali nell'ambito delle disposizioni dell'*AI Act*, salve specifiche eccezioni (cfr. anche considerando 2-*ter*, ove si chiarisce che l'*AI Act* non compromette l'applicazione delle vigenti norme UE che disciplinano il trattamento dei dati personali, compresi i poteri e le funzioni delle autorità di vigilanza indipendenti competenti per sorvegliare la conformità a tali regolamenti. Inoltre, l'*AI Act* non pregiudica il diritto fondamentale alla vita privata e alla protezione dei dati personali sancito dal diritto unionale in materia di protezione dei dati e dalla Carta dei diritti fondamentali dell'Unione Europea);
- art. 4-*bis*: prevede il dovere di sviluppare e utilizzare sistemi di AI in conformità alle normative sulla vita privata e protezione dei dati, garantendo al contempo la qualità e l'integrità dei dati stessi;
- art. 5, par. 1-*bis*: le restrizioni previste da altre leggi dell'Unione, comprese quelle sulla protezione dei dati, non vengono influenzate quando la produzione o l'impiego di sistemi di *AI* violi altre e differenti normative;
- art. 29, par. 6: gli operatori di sistemi di AI ad alto rischio utilizzano le informazioni fornite in osservanza all'articolo 13 (v. *retro*) per condurre una valutazione dell'impatto sulla protezione dei dati;
- art. 29-*bis*: prima di mettere in servizio un sistema di *AI* ad alto rischio, gli operatori devono condurre una valutazione dell'impatto dei sistemi

nel contesto specifico di utilizzo, tenendo conto di vari elementi, tra cui la conformità alle leggi in materia di diritti fondamentali;
- art. 63, par. 5: le autorità di controllo della protezione dei dati sono designate come autorità di vigilanza del mercato per i sistemi di *AI* utilizzati a fini di attività di contrasto, in conformità alla Direttiva (UE) 2016/680;
- Allegato VIII, sezione B: specifica le informazioni richieste per la registrazione dei sistemi di *AI* ad alto rischio, compresa una sintesi della valutazione dell'impatto sulla protezione dei dati ai sensi delle normative applicabili.

5. Conclusioni

Quanto sopra esposto evidenzia la necessità di un costante coordinamento tra la disciplina a tutela dei dati personali e quella in materia di regolazione dell'*AI*, essenziale al fine di assicurare una risposta efficace, anche in quanto aggiornata, alle esigenze di tutela sulle quali il GDPR e il venturo *AI Act* si fondano. Esigenza, questa, testimoniata anche dalla pubblicazione, da parte del CNIL francese, in data 16 ottobre 2023, di una consultazione specificamente dedicata alle questioni di allineamento tra GDPR e *AI Act*[12], nonché alla creazione di *data set* per l'*AI*, con la finalità di dimostrare come il GDPR costituisca fondamentale supporto a un "*approccio responsabile ed innovativo*" all'*AI*[13].

Riteniamo, inoltre, che, da parte degli operatori, un sistematico utilizzo di DPIA (art. 35 del GDPR) e di AIIA (art. 29 dell'*Ai Act*)[14], auspicabilmente da redigere congiuntamente, sia indispensabile per evitare una erronea valutazione dei rischi connessi alle singole applicazioni e sistemi di *AI*. E ricordiamo altresì che il GDPR (art. 35) già impone al titolare del trattamento l'effettuazione di DPIA nei casi in cui il trattamento dei dati "*prevede in particolare l'uso di nuove tecnologie*". Elevata attenzione deve poi essere posta nel contemperare le esigenze non perfettamente allineate di GDPR e *AI Act* in relazione alla qualità e natura dei dati. Se ai sensi dell'art. 10 dell'*AI Act* i *set* di dati di addestramento e, ove applicabile, i *set* di dati di convalida e prova devono essere pertinenti, sufficientemente rappresentativi, adeguatamente verificati e il più possibile completi alla luce della finalità prevista, per il GDPR i dati devono essere minimizzati, necessari e proporzionati (cfr. art. 5 del GDPR).

Non semplice appare, dunque, il compito del "produttore", così come dell'operatore, di sistemi di *AI* chiamato a garantire il rispetto di tutti i principi e le norme suscettibili di trovare applicazione in materia di *data protection*, tra

[12] https://www.cnil.fr/en/artificial-intelligence-cnil-opens-consultation-creation-datasets-ai
[13] https://www.cnil.fr/en/artificial-intelligence-cnil-unveils-its-first-answers-innovative-and-privacy-friendly-ai
[14] Ai sensi dell'art.29 ultimo comma della proposta di AI ACT. *Recommendations for Assessing AI Impacts to Human Rights, Democracy, and the Rule of Law, ECNL and Data&Society (2021) Critical Criteria for AI Impact Assessment: An Aggregated View, Civic AI Lab, University of Amsterdam (2023)* STAHL, B.C., ANTONIOU, J., Bhalla, N. ET AL. *A systematic review of artificial intelligence impact assessments*. *Artif Intell Rev* (2023). https://doi.org/10.1007/s10462-023-10420-8

GDPR e *AI Act*. Compito, per vero, reso indubbiamente più agevole dalla introduzione, nell'ultima versione della proposta di *AI Act*, di numerose norme di coordinamento tra quest'ultimo e GDPR[15]. Resta tuttavia indispensabile che l'attività di coordinamento tra i testi dei due regolamenti prosegua a livello operativo, evitando ogni disallineamento che sarebbe fonte di non secondarie problematiche applicative.

Tale attività di "manutenzione" ed interpretazione "autentica" a monte dovrà essere attuata a prescindere da quale soggetto svolgerà, in concreto, il ruolo di autorità competente per l'*AI*. Infatti, se in caso di creazione di un nuovo soggetto o di attribuzione delle funzioni ad un soggetto diverso dal Garante per la protezione dei dati personali, l'esigenza di coordinamento è particolarmente evidente, la stessa dovrà comunque avere luogo anche ove la competenza in materia di *AI Act* venisse attribuita al Garante stesso. Non sembra eccessivo affermare, al riguardo, che l'ampiezza degli ambiti applicativi dell'*AI* e la rilevanza degli interessi tutelati comporterebbero la necessità della creazione di una autonoma struttura interna al Garante, dotata di personale qualificato e dotato di competenze specifiche.

[15] Alle specifiche previsioni sopra citate valga aggiungere altresì l'emendamento 7 al considerando 2-*ter*, l'emendamento 53 al considerando 26-*quinquies*, ma soprattutto l'emendamento 80 al considerando 45-*bis*, che conferma la rilevanza del principio della minimizzazione dei dati e fornisce un criterio interpretativo generale per la corretta lettura dell'art. 10 dell'*AI Act*, ed in particolare del concetto di "sufficiente rappresentatività" dei dati.

Di Cerbo A, 'La tutela dell'identità nell'ambiente digitale alla luce delle norme europee' (2023) 2 EJPLT, 253 - 265.
DOI: https://doi.org/10.57230/EJPLT232ADC
ISSN 2704-8012



La tutela dell'identità nell'ambiente digitale alla luce delle norme europee

Identity protection in the digital environment in light of European Union regulations

ANTONELLA DI CERBO
Dottoranda in Diritto Civile Università degli Studi del Sannio
Funzionaria Autorità Garante per la protezione dei dati personali

Abstract
L'evoluzione tecnologica ed i riflessi che ha avuto sulla società hanno dato luogo al sorgere di nuove istanze di tutela, che con il tempo hanno trovato posto nelle carte sovranazionali e domestiche e che tutt'oggi sono al centro dell'attività parlamentare europea ed internazionale.
Dopo un excursus sull'affermazione di nuovi diritti attraverso il processo d'integrazione europea, il presente contributo analizza l'impatto dei regolamenti in materia di protezione dei dati personali e dei servizi digitali sul diritto all'identità digitale.

Technological evolution and its effects on society have given rise to new demands for protection, which over time have found their place into supranational and domestic charters and are still the focus of european and international parliamentary activity.
After a brief examination of the affirmation of new rights through the process of European integration, this paper analyzes the impact of data protection regulations and digital services on people's right to digital identity.

© The author(s) 2023, 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; Regolamento 2022/2065/UE; DSA; GDPR; Regolamento 679/2016/UE; identità digitale

Summary: Introduzione. – 1. Nuove istanze di tutela e nuovi diritti. – 1.1. Il riconoscimento di nuovi diritti nell'ordinamento domestico attraverso il processo d'integrazione europea. – 1.2 La tutela del diritto all'identità digitale ad opera del Regolamento 2016/679/UE. – 1.3 Il consenso come strumento di autodeterminazione informativa. – 2. Il Regolamento 2022/2065/UE. – 2.1. La responsabilità dei prestatori dei servizi. – 2.2. L'affermazione del diritto (condizionato) di accedere all'account social. – Conclusioni.

Introduzione.

Il presente contributo, formulato a titolo personale e senza alcun vincolo per l'Amministrazione di appartenenza (l'Ufficio del Garante), ha per oggetto la tutela dell'identità digitale, alla luce del nuovo quadro normativo: la disciplina del Regolamento 679/2016/UE e quella del Regolamento 2022/2065/UE.

Dallo studio dell'esperienza giuridica nazionale degli inizi del secolo scorso si registra sino agli anni settanta una tutela dell'identità della persona riferita essenzialmente ai segni distintivi, tramite il riconoscimento dei diritti al nome ed all'immagine di cui agli articoli 7 e 10 del codice civile; un'impostazione che rispondeva ad una lettura prettamente patrimoniale delle norme codicistiche ed abbandonata per lasciare spazio ad un'interpretazione costituzionalmente orientata delle stesse e fondata sulla valorizzazione della funzione sociale del diritto civile[1].

Parimenti, l'evoluzione tecnologica ed i riflessi che ha avuto sulla società ed il viver quotidiano delle persone hanno dato luogo al sorgere di nuove istanze di tutela che con il tempo hanno trovato posto nelle carte sovranazionali e domestiche e che tutt'oggi sono al centro dell'attività parlamentare del contesto europeo ed internazionale.

Le risposte legislative messe in campo sono inevitabilmente tardive: l'innovazione tecnologica è molto più rapida dell'intervento regolatore del legislatore, ciononostante è opportuno riconoscere e sottolineare che, ad oggi, la normativa europea rappresenta un modello di riferimento per tutto il mondo.

Gli atti comunitari analizzati nel presente contributo, in particolare i regolamenti in materia di protezione dei dati personali e dei servizi digitali, al

[1] P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, in Edizioni Scientifiche Italiane Spa, Napoli, 2020; P. Perlingieri, *La depatrimonializzazione e diritto civile,* in Rassegna di diritto civile Edizioni scientifiche italiane, Napoli, 1983; C. Donisi, *Verso la depatrimonializzazione del diritto privato*, in Rass.dir. civ. Edizioni scientifiche italiane, Napoli,1980; P. Perlingieri, *La dottrina del diritto civile nella legalità costituzionale*, in Rass. dir. civ., Napoli, 2007; P. Grossi, *La cultura del civilista italiano. Un profilo storico,* Giuffré Editore, Milano, 2002.

pari di quanto farà il regolamento in materia di intelligenza artificiale[2], rientrano tra i provvedimenti normativi più innovativi per la regolazione del settore tecnologico. Al contempo, grazie alla solida architettura giuridica europea eretta sul rispetto dei diritti e delle libertà fondamentali e dell'attività dei giudici dell'Unione, unità di interconnessione tra i sistemi giuridici nazionali[3], tali norme rappresentano strumenti di innalzamento della tutela in favore della persona.

1. Nuove istanze di tutela e nuovi diritti.

1.1. Il riconoscimento di nuovi diritti nell'ordinamento domestico attraverso il processo d'integrazione europea.

Il ruolo assunto dai diritti e dalle libertà affermati nella prima parte della carta costituente ha portato al riconoscimento, tramite l'articolo 2 della costituzione di nuovi diritti, tra cui il diritto alla protezione dei dati personali ed il diritto alla riservatezza, con ciò rivelando un'incredibile lungimiranza dei padri costituenti.

Si tratta di situazioni giuridiche sancite dalle carte sovranazionali, in primis dalla Convenzione europea dei diritti dell'uomo, che afferma il diritto di ogni persona "al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza" e, a livello europeo, dalla Carta di Nizza, ove i diritti in argomento, sono disciplinati dagli articoli 7 ed 8 e costituiscono, a seguito del Trattato di Lisbona, il parametro di riferimento costituzionale in materia di diritti fondamentali nel contesto unionale.

Nell'ordinamento interno tali norme vengono astrattamente collocate tra la Costituzione e le leggi ordinarie, assumendo i connotati ed il valore delle norme interposte ed integrando la carta costituente, con la conseguenza che la loro osservanza è imposta sia al legislatore sia ai giudici nazionali, che sono tenuti a disapplicare le disposizioni domestiche in contrasto con l'acquis comunitario, favorendo la realizzazione della tutela multilivello dei diritti a cui tende il processo d'integrazione europeo. Dai primi anni 90 la Corte di Giustizia è altresì giunta ad affermare che, al pari del giudice, tutte le amministrazioni nazionali hanno l'obbligo di applicare le disposizioni di una direttiva[4].

Ciò avviene in quanto, diversamente dagli obblighi di diritto internazionali, quelli derivanti dalla normativa comunitaria, non necessitano di un atto di recepimento da parte degli Stati membri, specie se si tratta di atti immediatamente esecutivi come i regolamenti e le direttive self executing[5].

---

[2] Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, Bruxelles, 06.03.2024 (In attesa di pubblicazione in Gazzetta Ufficiale).

[3] O. POLLICINO, *Costruendo le tradizioni dei diritti in Europa: il senso di un gerundio, e di un seminario,* Seminario annuale di diritti comparati, Macerata, 2015

[4] Corte di giustizia (C103/88), 22.6.1989 in in *Eur-Lex*;

[5] Corte di Giustizia (C193/91), 25 .05.1993, in *Eur-Lex*; Corte di Giustizia (C6/90 e C 9/90), 19 .11.1991, in *Eur-Lex.*

L’efficacia obbligatoria delle norme comuni nell’ordinamento interno è stata resa possibile alla luce dell’articolo 11 della costituzione, seppur in assenza di un espresso riferimento alla realtà comunitaria, ed è divenuta concretamente esecutiva tramite la formulazione delle dottrine del primato del diritto dell’Unione e dell’effetto diretto ad opera della Corte di giustizia dell’Unione europea.

La legittimità del ricorso all’articolo 11 della costituzione, per giustificare le cessioni di sovranità, rappresenta ancora oggi una questione controversa. La dottrina prevalente ritiene che il processo di creazione dell’Unione e la redazione della carta fondamentale dell’ordinamento italiano siano parte del medesimo progetto giuridico: la costituzione del 1948 nasce nello stesso spirito e nella stessa epoca in cui sono piantati i primi semi dell'unione europea (CECA). Mentre la dottrina minoritaria[6] ritiene che dai lavori preparatori dell’Assemblea costituente e da una lettura fedele del testo dell’articolo 11, che contempla limitazioni di sovranità da parte dell’ONU al sol fine di creare meccanismi di risoluzione delle controversie idonei a disinnescare, ex ante, il rischio di futuri contrasti mondiali, sia chiaro che il ricorso alla norma in argomento sia frutto di una manipolazione interpretativa.

La Corte costituzionale ha da tempo accolto il primo orientamento riconoscendo all’articolo 11 il fine di "porre le fondamenta di una unione sempre più stretta tra i popoli europei", diretta "ad assicurare mediante un'azione comune il progresso economico e sociale dei loro paesi, eliminando le barriere che dividono l'Europa", e ciò nel preciso intento di "rafforzare le difese della pace e della libertà, facendo appello agli altri popoli d'Europa, animati dallo stesso ideale, perché si associno al loro sforzo", nonché di "confermare la solidarietà che lega l'Europa ai paesi d'oltremare, desiderando assicurare lo sviluppo della loro prosperità conformemente ai principi dello Statuto delle Nazioni Unite"[7].

La norma in argomento è ancora oggi invocata per consentire le limitazioni introdotte dai trattati comunitari relativamente all’attività legislativa, amministrativa e giurisdizionale, non essendo mai intervenuta una riforma costituzionale in tal senso.

La carta fondamentale italiana è aperta all'Europa e la Corte costituzionale, in quanto garante, è tenuta a garantire il rispetto anche delle norme europee[8].

Il processo d’integrazione europeo avviato da tali premesse è stato favorito dall’elaborazione delle dottrine di matrice giurisprudenziale del primato del diritto dell’Unione europea e dell’effetto diretto; la Corte di giustizia, sin dall'inizio del processo di interpretazione del diritto dell'Unione, ha ritenuto fondamentale conferire un ruolo di primo piano al diritto europeo escludendo deroghe statali.

Nel corso del lungo cammino comunitario la Corte costituzionale ha però affermato che la prevalenza del dettato comunitario non è senza limiti,

---

[6] G. PALMA, *L’incompatibilità tra costituzione italiana e trattati dell’unione europea. I principali aspetti di criticità,* 2015, in Diritto.it

[7] Corte Cost. 18.12.1973, n.183, pag.3, in il *Foro Italiano.*

[8] Corte costituzionale, *I diritti fondamentali nell’ordinamento giuridico comunitario e negli ordinamenti nazionali*, 2017, in Servizio studi della Corte costituzionale. Consultabile online: https://www.cortecostituzionale.it/documenti/convegni_seminari/STU_306_Diritti_fondamentali_2017.pdf

precisando che, i giudici nel garantire la piena applicazione del diritto europeo devono tener conto dei limiti posti dai principi propri del tessuto della carta costituente: i principi fondamentali, che costituiscono controlimiti alle limitazioni di sovranità e che sono sottratti alla procedura di revisione costituzionale. Limitazioni di sovranità e controlimiti segnano lo spazio dell'unificazione giuridica europea consentita dalla costituzione italiana[9].

1.2. La tutela del diritto all'identità digitale ad opera del Regolamento 2016/679/UE.

Il progressivo cambio del paradigma condotto attraverso la valorizzazione dei diritti e delle libertà fondamentali ha consentito un notevole accrescimento della portata del diritto all'identità personale, in linea con le nuove istanze di tutela che la rivoluzione tecnologica ha prodotto nel tempo.

Le nuove tecnologie hanno profondamente modificato il viver quotidiano e le relazioni sociali, creando uno spazio virtuale in cui la persona è frammentata in molteplici identità. La Rete da mezzo è divenuto mondo, orizzonte prevalente dell'agire umano in cui si iscrivono le coordinate della vita pubblica e privata[10].

In tale contesto il diritto alla protezione dei dati personali rappresenta il principale strumento di tutela di cui dispone la persona per avere il controllo delle proprie informazioni, scegliere quali parti di sè rendere note alla generalità dei consociati e ricomporre l'io diviso per avere una rappresentazione della sua persona nella sua integrità[11].

La normativa in materia di protezione dei dati personali di derivazione comunitaria è stata introdotta nell'ordinamento nazionale mediante la Direttiva n.95/ 46, oggi sostituita dal Regolamento europeo, sostituzione che ha reso necessaria, ad opera del d.lgs n.101/2018, una revisione del codice della privacy.

Gli articoli da 15 a 22 del Regolamento in argomento attribuiscono all'interessato il diritto di accedere alle proprie informazioni, di chiederne la rettifica, di opporsi al trattamento dei dati personali ovvero, laddove sussistano i presupposti, di ottenere la cancellazione dei suoi dati. L'articolo 22 prevede altresì il divieto, derogabile solo nei casi previsti dal paragrafo 2 della stessa norma, di trattare dati personali per adottare decisioni completamente automatizzate.

---

[9] Corte costituzionale, *Le limitazioni della sovranità statale in favore dell'Unione europea nella giurisprudenza costituzionale. Il sistema delle fonti.* in Servizio studi della Corte costituzionale. 2014. Consultabile online: https://www.cortecostituzionale.it/documenti/convegni_seminari/STU_262.pdf ; R. BIN, *È scoppiata la "terza guerra tra le Corti"? A proposito del controllo esercitato dalla Corte di cassazione sui limiti della giurisdizione,* in Federalismi.it, 2020; M. CARTABIA, *"Unità nella diversità": il rapporto tra la Costituzione europea e le Costituzioni nazionali*, in Il diritto dell'Unione europea, n. 3, 2005; A. LO CALZO, "*Dagli approdi giurisprudenziali della Corte costituzionale in tema di controlimiti alle recenti tendenze nel dialogo con le Corti nel contesto europeo*", in Federalismi.it, 2022.

[10] A. SORO, *Intervento del Presidente Antonello Soro, Presidente dell'Autorità Garante per la privacy* I confini del digitale, Atti del convegno *I confini del digitale. Nuovi scenari per la protezione dei dati*, Roma, 2019. Consultabile online: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9078531

[11] S. RODOTÀ, *Una costituzione per Internet?,* Politica del diritto, Fascicolo 3, in Il Mulino – Rivistaweb., 2010

Si tratta di diritti che offrono una tutela in forma specifica in un'ottica di valorizzazione del principio di autodeterminazione informativa e la cui violazione consente l'esercizio dei poteri correttivi da parte dell'autorità di controllo di cui all'articolo 58, par. 2, del Regolamento, che consistono nella possibilità di rivolgere al titolare o al responsabile avvertimenti, ammonimenti, ovvero di ingiungere loro di soddisfare le richieste dell'interessato di esercitare i diritti, di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine e di comunicare all'interessato una violazione dei dati personali. L'autorità ha altresì i poteri di imporre una limitazione provvisoria o definitiva al trattamento, ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento, revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a infliggere una sanzione amministrativa pecuniaria, nonché di ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Al netto della tutela rimediale, l'intero impianto normativo del Regolamento generale in materia di protezione dei dati personali garantisce la tutela della persona attraverso obblighi che incombono sul titolare in via preventiva e che sono modellati sulle specifiche attività di trattamento che svolge, quindi sui rischi specifici derivanti dalle stesse, in virtù del principio di accountability di cui all'articolo 5, par. 2, del Regolamento. Ne consegue che il titolare è tenuto a strutturare le attività che coinvolgono i dati personali in modo da assicurare, sin dalla progettazione e per impostazione predefinita, il rispetto dei principi generali e delle norme fissati dalle discipline europea e nazionale.

Tramite un approccio sostanzialistico di tipo preventivo il regolamento favorisce l'adozione di una strategia aziendale su misura ed al contempo traccia il limite oltre il quale l'iniziativa economica deve cedere il passo alla tutela della persona.

Con l'ingresso nella normativa unionale del Regolamento ogni formalismo che consentiva di ricondurre (e ridurre) gli obblighi del titolare a meri adempimenti burocratici è stato definitivamente abbandonato.

Dalle relazioni annuali dell'Autorità di controllo emerge un ampio ricorso ai diritti di cui al Capo III del Regolamento, in particolare al diritto alla cancellazione dei dati personali, che rappresenta il principale strumento per impedire la diffusione di informazioni nel contesto online, in cui le istanze di tutela della identità digitale e quella personale si sovrappongono.

L'esperienza giuridica rivela che le autorità preposte alla tutela della persona considerino tale diritto una prerogativa relativa da contemperare con diritti di pari rango; ciò onde evitare che una situazione giuridica si atteggi in modo tiranno e goda di un'ingiustificata iperprotezione.

La contesa tra il diritto alla identità personale ed il diritto alla libertà di manifestazione del pensiero è particolarmente evidente nel contesto giornalistico, ambito in cui sono infatti previste espresse deroghe (assistite da altrettanti limiti) alla disciplina generale. Come chiarito anche dalla Corte costituzionale, la composizione di tale contrasto deve avvenire attraverso l'abbandono di soluzioni precostituite che prediligano la costante prevalenza di un diritto su un altro, lasciando spazio ad un delicato bilanciamento che tenga

conto delle circostanze del caso concreto e che sia condotto alla stregua dei principi generali, in primo luogo quelli di minimizzazione e di finalità del trattamento sanciti dagli articoli 5, par.1, lett. b) e c).

La giurisprudenza europea e nazionale ha in più occasioni individuato una soluzione di compromesso tra i diritti alla riservatezza ed alla protezione dei dati personali ed il diritto alla libertà di informazione nella deindicizzazione dei dati personali dell'interessato, in modo tale che, da un lato, le notizie di cui venga richiesta la cancellazione non siano immediatamente a lui riconducibili attraverso una ricerca (mediante query) che parta dal suo nome, e, dall'altro, l'interesse conoscitivo della generalità dei consociati sia comunque soddisfatto.

Da un'altra prospettiva si osserva che, nel contesto online, il diritto alla libertà di manifestazione del pensiero di cui all'articolo 21 della carta costituzionale, inteso nella sua accezione più ampia, sia frequentemente minato dagli algoritmi che governano la rete e che rinchiudono l'interessato in camere dell'eco caratterizzate dalla presenza di contenuti in linea con le preferenze da lui espresse attraverso un susseguirsi di click.

Il pedinamento digitale, ad opera di strumenti di tracciamento online come i cookie, si colloca tra le pratiche più pericolose per l'integrità del diritto alla identità personale digitale, in quanto capace di condizionare l'autodeterminazione dei singoli e le loro opinioni, che, infatti, risultano sempre più polarizzate.

La pratica di queste attività è oggi ammessa e subordinata alla (sola) raccolta preventiva del consenso libero, informato, specifico ed inequivocabile dell'interessato.

1.3 Il consenso come strumento di autodeterminazione informativa.

Il quadro giuridico che regola l'utilizzo ed il funzionamento dei cookie e degli altri strumenti di tracciamento online è costituito dal Regolamento generale, nonché dalle disposizioni della Direttiva 2002/58/CE (c.d. direttiva e-Privacy) relativa alla vita privata e alle comunicazioni elettroniche, recepite nell'ordinamento nazionale con l'art. 122 del Codice privacy.

Per quanto concerne l'interazione tra le due normative il comitato europeo dei garanti ha chiarito che[12] le disposizioni della direttiva e-Privacy precisano quelle del regolamento per quanto riguarda il trattamento dei dati personali nel settore delle comunicazioni elettroniche e che, in conformità con il principio *lex specialis derogate legi generali*, le prime prevalgono sulle seconde nelle situazioni che intendono disciplinare in modo specifico. Di contro, qualsiasi trattamento di dati personali non specificamente disciplinato dalla direttiva e-Privacy rimane soggetto alle disposizioni del regolamento.

L'articolo 4, numero 11, del regolamento in materia di dati personali definisce il consenso come "qualsiasi manifestazione di volontà libera,

[12] European Data Protection Board (EDPB), *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities,* 2019; E. NUNZIANTE, *Rapporto tra direttiva e privacy e GDPR: l'opinione dei Garanti Ue*, in Agenda Digitale, 2019

specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

I requisiti del consenso sono specificati nell'articolo 7 del Regolamento e, più dettagliatamente, nelle linee guida n.5/2020[13] adottate dal Comitato europeo, secondo cui il consenso, per essere valido, deve essere specifico, al fine di evitare che venga utilizzato per le attività di trattamento di volta in volta individuate dal titolare e non corrispondenti a quelle illustrate nell'informativa, nonché libero. Non è rispondente a tale ultimo requisito la volontà positiva espressa dall'interessato che si trovi a scegliere tra la cessione dei suoi dati personali e la rinuncia del servizio (take it or leave it). La volontà della persona appare tanto più frustrata se si considerano, ai fini dello scambio, quei servizi che consentono l'esercizio di diritti fondamentali, come la posta elettronica rispetto al diritto alla corrispondenza garantito all'articolo 15 della costituzione.

In attesa che l'Autorità garante si pronunci[14], le uniche risposte in merito provengono dalla Corte europea che ha chiarito che, dinanzi all'opzione take it or leave it, il consenso sia da ritenersi coartato, salvo che lo stesso titolare offra servizi equivalenti di cui l'interessato possa fruire anche senza cedere i propri dati personali[15].

2. Il Regolamento 2022/2065/UE.

2.1. La responsabilità dei prestatori dei servizi.

Gli obiettivi di autodeterminazione informativa e di tutela dell'identità digitale della persona sono perseguiti altresì dal Regolamento (UE) 2022/2065 (d'ora in poi DSA)[16] relativo al mercato unico dei servizi digitali, che modifica la direttiva 2000/31/CE, inserendosi nel complesso quadro della strategia digitale europea.

L'articolo 26 del DSA rubricato "Pubblicità sulle piattaforme online regola le attività pubblicitarie sulle piattaforme online, ampliando la sfera giuridica dei destinatari dei servizi digitali attribuendo loro il diritto di essere messi in grado di identificare in modo chiaro, conciso, inequivocabile ed in tempo reale "che l'informazione costituisce una pubblicità; la persona fisica o giuridica per conto della quale viene presentata la pubblicità; la persona fisica o giuridica che paga

[13] European Data Protection Board (EDPB), *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 2020.

[14] Garante per la protezione dei dati personali, *Cookie wall: prosegue l'istruttoria del Garante privacy su alcune testate giornalistiche online,* 2022, Consultabile online: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9822601

[15] Corte di giustizia (673/17-Planet49), 1 ottobre 2019, in *Eur-Lex*; R. COBAZZI, *Utilizzo dei cookie e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di giustizia nel caso Planet49,* in Medialwas, 2020*;* M. C. MENEGHETTI, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy,* in Medialwas, 2021

[16] Regolamento 2022/2065/UE

per la pubblicità, se detta persona è diversa dalla persona fisica o giuridica di cui alla lettera; le informazioni rilevanti direttamente e facilmente accessibili dalla pubblicità relative ai parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità e, laddove applicabile, alle modalità di modifica di detti parametri".

Parimenti, l'articolo 27 rubricato "Trasparenza dei sistemi di raccomandazione" mira a garantire la massima trasparenza in favore dei consumatori e riequilibrare, seppur parzialmente, l'asimmetria informativa che caratterizza i rapporti business to consumer (B2C) prevedendo in favore dei destinatari dei servizi online un diritto innovativo, che si presume avrà un significativo impatto nel contesto digitale: il diritto di chiedere la modifica dei criteri sulla base dei quali avviene la personalizzazione dei contenuti che vengono mostrati all'utente. I gestori delle piattaforme che si avvalgono di sistemi di raccomandazione saranno tenuti a specificare nelle condizioni generali di utilizzo del servizio, in un linguaggio chiaro e intellegibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché le ragioni per cui talune informazioni sono loro suggerite. Unitamente a tale diritto, il DSA prevede che siano offerte ai fruitori dei servizi digitali delle opzioni di scelta che consentano loro di modificare i parametri impostati di default ai fini della determinazione dei sistemi di raccomandazioni, anche attraverso una sezione specifica dell'interfaccia della piattaforma. Tale funzionalità dovrà essere sempre disponibile all'utente, consentendogli di selezionare e modificare l'opzione preferita in qualsiasi momento, così determinando liberamente ed autonomamente le informazioni a cui dare priorità.

La trasparenza ed il controllo sottesi a tale previsione rimarcano quanto già previsto dall'articolo 22 del Regolamento in materia di protezione dei dati personali in punto di processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione, e dal considerando 71 della stessa normativa che recita "Tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore".

In continuità con il suddetto considerando, il legislatore del DSA, consapevole dei rischi della profilazione e dell'impatto che può avere sul grado di sviluppo ed autoconsapevolezza dei minori, vieta ex articolo 28, par.2,[17] ogni tipo di attività di profilazione basata sui dati personali dei minori ed individua tale trattamento tra i rischi sistemici significativi di cui le piattaforme di dimensioni molto grandi devono tener conto ai fini dell'individuazione di misure tecniche ed organizzative adeguate, nonché nell'ambito degli audit indipendenti a cui devono periodicamente sottoporre la loro attività.

In particolare, con riferimento alle c.d. Large Online Platforms - LoPs - di cui all'articolo 34, par.1, lett. d) del DSA, la normativa richiede che nel valutare i rischi sistemici si tenga conto di "qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute

pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona".

La lettura del DSA suggerisce ulteriori considerazioni in ordine alla tutela dell'identità della persona nell'ambiente digitale.

In particolare, per quanto concerne la responsabilità dell'Hosting provider si rammenta che la Direttiva 2000/31 prevedeva *ex* articoli 12-15 (oggi espressamente soppressi dall'articolo 89 del DSA) un discusso regime di (ir)responsabilità dei prestatori dei servizi, secondo cui tali soggetti venivano esonerati da responsabilità in presenza di determinate condizioni, essendo escluso nei loro riguardi un obbligo generale sia di sorveglianza sulle informazioni che trasmettono o memorizzano che di accertamento attivo dei fatti o delle circostanze che indichino la presenza di attività illegali.[18]

La disciplina era completata dal decreto d.lgs. n. 70 del 2003, attuativo della Direttiva 2000/31, ove l'articolo 16 prevedeva la responsabilità in capo al prestatore dei servizi che non avesse provveduto alla immediata rimozione dei contenuti illeciti ovvero che avesse continuato a pubblicarli, pur in presenza delle seguenti condizioni: conoscenza legale dell'illecito perpetrato dal destinatario del servizio, a seguito di una comunicazione da parte del titolare del diritto leso ovvero in quanto appreso *aliunde*; evidente l'illiceità dell'altrui condotta, laddove fosse imputabile all'hosting provider una colpa grave per non averla positivamente riscontrata; ciò alla stregua del grado di diligenza ragionevolmente atteso da un operatore professionale della rete in un determinato momento storico; possibilità concreta di attivarsi utilmente, in quanto edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere".[19]

Parte della dottrina e della giurisprudenza[20] hanno a lungo adottato un'interpretazione *sui generis* delle suddette norme, operando una distinzione tra due figure di hosting provider in realtà non rinvenibile nel dettato normativo, secondo cui il regime di favore stabilito dal d.lgs. 70/2003 non trova applicazione in presenza di un provider che completi e arricchisca in modo non passivo la fruizione dei contenuti da parte degli utenti, attraverso operazioni di: filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione, promozione dei contenuti; ovvero l'impiego di strumenti di valutazione del comportamento degli utenti.

Viceversa, secondo tale impostazione, l'hosting provider passivo, autore di una un'attività di prestazione di servizi neutra, di ordine meramente tecnico, automatico e, pertanto, non in grado di esercitare alcun controllo sulle informazioni trasmesse o memorizzate dai destinatari dei suoi servizi, è esente da responsabilità[21].

---

[18] Cass.civ.,19.03.2019, n. 7708, par. 5.1, in *Italgiure Web;* D. IASELLI*, Responsabilità del provider: la Cassazione detta rilevanti principi di diritto, Cassazione civile, sez. I, sentenza 19/03/2019 n° 7708,* in Altalex, 2019; C. D'ONOFRIO, *La Cassazione si pronuncia sulla responsabilità di un hosting provider attivo e sul risarcimento del danno,* in Diritto al digitale, 2022; T.A.R. Lazio Roma Sez. IV, 24 gennaio 2024, n. 1393

[19] Cass. pen., 17.12.2013 n.3672 *in Italgiure Web.*; Cass. civ., 16.09.2021, n. 25070, in *Italgiure Web.*

[20] Cass., 19.03.2019, n.7708, in *in Italgiure Web*

[21] Corte di giustizia (C-291/13), 11.09.2014 in *Eur-Lex;* Corte di giustizia (C-324/09), 12.07.2011 in *Eur-Lex.;* C. D'URSO*, I profili informatici nella valutazione della responsabilità dell'Hosting Provider*, 2021, in Rivista Italiana di Informatica del Diritto.

Con il DSA, operativo dal 17 febbraio 2024, il legislatore europeo chiarisce i dubbi del passato prevedendo un chiaro quadro per l'esenzione condizionata dalla responsabilità dei prestatori di servizi intermediari, in particolare affermando all'articolo 8, collocato nel Capo II titolato "Responsabilità dei prestatori di servizi intermediari", che "ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali" e precisa ai considerando 21 e 22 che "un prestatore dovrebbe poter beneficiare delle esenzioni dalla responsabilità per i servizi di semplice trasporto e memorizzazione temporanea se non è in alcun modo coinvolto nelle informazioni trasmesse o alle quali è stato fatto accesso. A tal fine è necessario, tra l'altro, che il prestatore non modifichi le informazioni che trasmette o alle quali fornisce accesso. Tale prescrizione non dovrebbe tuttavia intendersi riferita alle manipolazioni di carattere tecnico effettuate nel corso della trasmissione o dell'accesso, purché tali manipolazioni non alterino l'integrità delle informazioni trasmesse o alle quali è fornito accesso." "Al fine di beneficiare dell'esenzione dalla responsabilità per i servizi di memorizzazione di informazioni, il prestatore dovrebbe agire immediatamente per rimuovere le attività illegali o i contenuti illegali o per disabilitare l'accesso agli stessi non appena ne venga effettivamente a conoscenza o ne divenga consapevole."

L'atto europeo afferma dichiaratamente che le esenzioni dalla responsabilità dovrebbero applicarsi in relazione a qualsiasi tipo di responsabilità per ogni tipo di contenuto illegale, indipendentemente dall'oggetto preciso o dalla natura esatta di tali leggi[22]; ciò in quanto il problema dei contenuti e delle attività illegali online non dovrebbe essere affrontato concentrandosi esclusivamente sulla loro responsabilità e sulle loro competenze ma coinvolgendo anche attori, tra cui i moderatori dei gruppi negli ambienti online chiusi, limitando il coinvolgimento degli intermediari solo laddove dispongano, effettivamente, della capacità tecnica e operativa per contrastare contenuti illegali.[23]

Ad ogni modo, trattandosi di una esenzione condizionata, la stessa non trova applicazione laddove il destinatario del servizio agisca sotto l'autorità o il controllo del prestatore di servizi di memorizzazione di informazioni. Ad esempio, nel caso in cui il fornitore di una piattaforma online consenta ai consumatori di concludere contratti a distanza con operatori commerciali, definendo il prezzo dei beni o dei servizi, ovvero qualora lo stesso collabori deliberatamente con il destinatario dei servizi al fine di commettere attività illegali.

2.2 L'affermazione del diritto (condizionato) di accedere all'account social.

Il DSA regola altresì il regime applicabile ai provvedimenti adottati dai fornitori a seguito della violazione da parte del destinatario del servizio degli

[22] Considerando 17 Reg. 2022/2065/UE
[23] Considerando 27 Reg. 2022/2065/UE

standard della community o della diffusione di contenuti illegali, introducendo una maggiore trasparenza in favore degli utenti. Si tratta di provvedimenti che dispongono: restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; la sospensione o la cessazione totale o parziale della prestazione del servizio ovvero la a sospensione o la chiusura dell'account del destinatario del servizio.

Le novità normative confermano l'importanza delle piattaforme social: vere e proprie comunità parallele, ove trova espressione l'identità personale dell'individuo ed in cui vengono instaurate relazioni sociali e professionali[24].

Il DSA introduce nella sezione 2 obblighi aggiuntivi applicabili ai prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online, che mirano, da un alto, a preservare la sicurezza dell'ambiente digitale e, dall'altro, a rendere edotto il destinatario di un provvedimento di restrizione, sospensione o blocco dell'account.

In particolare l'articolo 16 della normativa in argomento richiede ai prestatori di servizi di memorizzazione di informazioni l'introduzione di meccanismi che permettano agli utenti di segnalare la presenza di contenuti che ritengano in contrasto con i termini e le condizioni di utilizzo del servizio. Le segnalazioni devono essere precise ed adeguatamente motivate.

A tutela del titolare dell'account del destinatario del servizio, l'articolo 17 del DSA prevede che i fornitori instaurino un dialogo con l'utente segnalato affinché questo sappia, attraverso una motivazione chiara, che specifichi in che modo i contenuti caricati sulla piattaforma siano incompatibili con le condizioni generali del servizio ovvero illegali.

Tali questioni meritano di essere esaminate anche in considerazione delle pretese risarcitorie che potrebbero legittimante vantare i titolari di un account destinatari di provvedimenti che ne impediscano, ingiustificatamente, la piena fruibilità, con evidenti lesioni della loro sfera giuridica. Tra i primi interventi giurisprudenziali sul punto si segnala la pronuncia con cui il Tribunale Ancona[25] ha recentemente statuito che "prima di procedere alla disabilitazione definitiva dell'iscrizione di un utente ad un social network s'impone, al fornitore del servizio, una puntuale verifica delle violazioni contrattuali, stante che ciò comporta la cancellazione definitiva dei dati associati all'account, con la conseguenza che, altrimenti, si avrebbe una lesione dell'identità digitale e una responsabilità contrattuale (…) alla quale consegue un risarcimento del danno alla persona, in questo caso digitale, risarcimento ancor più consistente allorquando l'account non è più ripristinabile e sono stati distrutti i dati personali ad esso collegati."

[24] A. AMIDEI, *Tutela del consumatore – Il vaglio di validità delle clausole contrattuali di content moderation online,* in Giur.It., 2023; S. FLAMINIO, *Lotta alle fake news: dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Sercvice Act*, in Rivista italiana di informatica e diritto, Fascicolo 2, 2002
[25] Tribunale Ancona Sez.I, 15.06.2023, pag.1, in Leggi d'Italia

Conclusioni.

Le garanzie introdotte dal nuovo regolamento in materia di servizi digitali si inseriscono, unitamente a quelle previste dal regolamento in materia di protezione dei dati personali, nella sfida europea di coniugare dignità e innovazione nella consapevolezza di non poter demandare a protocolli informatici o contrattuali, unilateralmente stabiliti dai big tech, la disciplina del contesto, quello digitale, in cui più di ogni altro si dispiega la nostra esistenza[26].

Le piattaforme hanno acquisito un potere tale da sopravanzare perfino quello statale, ridisegnando con le condizioni del contratto il perimetro dell'esercizio dei diritti e delle libertà fondamentali[27].

È in tale contesto che lo Stato, anche attraverso l'attività delle Autorità di controllo, è chiamato a riappropriarsi del ruolo di garante del rispetto dei diritti fondamentali.

[26] A. SORO, *Proteggere i dati per governare la complessità*, Relazione Autorità garante per la protezione dei dati personali, Roma, 2017: A. VERCELLOTTI, *Reputazione online, come difenderla? Guida pratica per aziende e professionisti,* in Agenda Digitale, 2022

[27] P. STANZIONE, *Relazione introduttiva. Il Metaverso tra utopie e distopie*, in atti del Convegno *Il Metaverso tra utopie e distopie. Orizzonti e sfide della protezione dei dati,* Roma, 2023, 13. Consultabile online: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9939113

LIST OF AUTHORS OF THIS EJPLT ISSUE

ATTILIO ALTIERI – Research Fellow in Business Law, University of Foggia, Foggia, Italy.

LIVIA AULINO – Ph.D., Senior Researcher of the Research Centre in European Private Law (ReCEPL), Suor Orsola Benincasa University of Naples, Naples, Italy. Post-doc in Private Law, University of Naples Federico II, Naples, Italy.

ANDREA BORRONI – Associate Professor of Comparative Law, University of Campania Luigi Vanvitelli, Santa Maria Capua Vetere, Italy.

ILARIA AMELIA CAGGIANO – Full professor of Private Law, Suor Orsola Benincasa University of Naples, Naples, Italy. Vice-director of the Research Centre in European Private Law (ReCEPL), Suor Orsola Benincasa University of Naples, Naples, Italy.

ROBERTO CARLEO – Full Professor of Private Law, Parthenope University of Naples, Naples, Italy. Barrister.

ROBERTO CASO – Full Professor of Comparative Private Law, University of Trento, Trento, Italy.

JACOPO CIANI SCIOLLA – Researcher in Philosophy of Law and Legal Informatics, University of Turin, Turin, Italy. Adjunct Professor at ESCP, Turin Campus, Turin, Italy. Fellow of the Information Society Law Center, University of Milan, Milan, Italy.

IRENE COPPOLA – Research Fellow in Private Law, University of Naples Federico II, Naples, Italy.

LUCILA INÉS CÓRDOBA – Associate Professor of Family and Succession Law, University of Buenos Aires, Buenos Aires, Argentina.

ANTONELLA DI CERBO – Ph.D. Student of Civil Law, Sannio University, Benevento, Italy. Official of Italian Data Protection Authority.

MARIA CRISTINA GAETA – Lecturer in Private Law, Ph.D., Suor Orsola Benincasa University of Naples, Naples, Italy. Scientific Secretary of the Research Centre in European Private Law (ReCEPL), Suor Orsola Benincasa University of Naples, Naples, Italy.

LUCILLA GATT – Full professor of Private Law, Suor Orsola Benincasa University of Naples, Naples, Italy. Director of the Research Centre in European Private Law (ReCEPL), Suor Orsola Benincasa University of Naples, Naples, Italy.

PAOLA GRIMALDI – Lecturer, Assistant Professor of Private Law, University of Campania Luigi Vanvitelli, Santa Maria Capua Vetere, Italy.

ANTONGIULIO LOMBARDI – Expert of Law&Tech.

GIANLUCA MONTANARI VERGALLO – Associate Professor of Legal Medicine, Sapienza University of Rome, Rome, Italy.

ADRIANA SYLVINA MÓRON – Lecturer of Private Law, Università Abierta Interamericana, Buenos Aires, Argentina.

ABIGAIL OWUSU – Postdoctoral Research Fellow, University of Verona, Verona, Italy. Lawyer.

UGO PAGALLO – Full Professor of Philosophy of Law, Law and Technology and Legal Theory, University of Turin, Turin, Italy. Member of the Nexa Center for Internet and Society Board of Trustees.

PASQUALE RICCI – Ph.D. in Social and Forensic Medicine, Sapienza University of Rome, Rome, Italy.

ROBERTO SENIGAGLIA – Full Professor of Private Law, Ca' Foscari University of Venice, Venice, Italy.

EMILIO TOSI – Associate Professor of Private Law, Bicocca University of Milan, Milan, Italy. Executive Director, Centro Studi "Diritto Nuove Tecnologie".

EMILIANO TROISI – Ph.D., Junior Researcher of the Research Centre in European Private Law (ReCEPL), Suor Orsola Benincasa University of Naples, Naples, Italy.

FRANCO TRUBIANI – Researcher in Private Law, Parthenope University of Naples, Naples, Italy.

FABIO ZAMBARDINO – Post-doctoral fellow, University of Campania Luigi Vanvitelli, Santa Maria Capua Vetere, Italy.